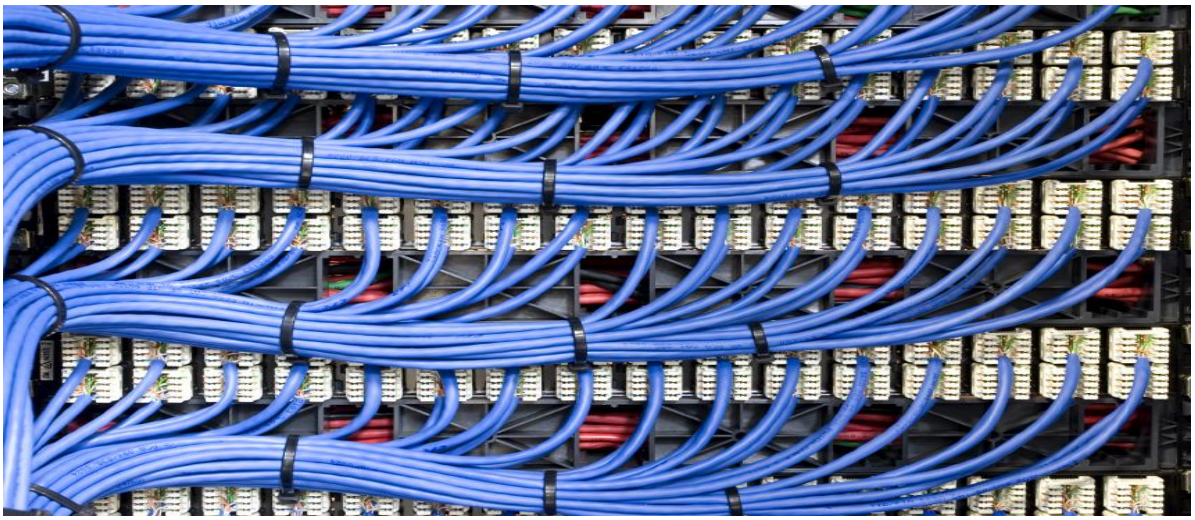
NSS 122 (NETWORK CABLING)



CABLING

Cabling is the set of wires made of either copper or glass that is used to connect computers and other network components to enable them to communicate, thus forming a network of computers.

WHAT IS NETWORK CABLING?

In other words, Network Cabling is the medium through which information usually moves from one network device to another. There are several types of cable which are commonly used with LANs. In some cases, a network will utilize only one type of cable, other networks will use a variety of cable types. The type of cable chosen for a network is related to the network's topology, protocol, and size. Understanding the characteristics of different types of cable and how they relate to other aspects of a network is necessary for the development of a successful network.

Laying cables is the foundation for both creating local area networks (LANs) and connecting LANs into wide area networks (WANs).

CAT 6 networking cabling.

NETWORK CABLE TYPES AND SPECIFICATIONS

Network cables specifications, standards, and features of the coaxial cable, twisted-pair cable, and the fiber-optical cable would be outlined below: -

To connect two or more computers or networking devices in a network, network cables are used. There are three types of network cables namely: -

- Coaxial cable
- Fiber-optic cable and
- Twisted-pair cable.

COAXIAL CABLE

Coaxial cables are a form of signal transmission cable that is used to pass electrical signals between devices, systems, or components. Whereas standard electrical cable consists of one or more wires through which an electrical current is passed (a flow of electrons), coaxial cable is used to pass radio frequency (RF) signals in the form of a transverse electromagnetic wave. The design of coaxial cable consists of an inner conductor surrounded by a dielectric layer, which is then enclosed in a cylindrical sandwich that contains additional layers of shielding as well as an outer protective jacket to prevent damage to the signal carrying components during installation or from environmental stresses. Coaxial cables are commonly used as transmission lines and can transmit high-frequency signals at low loss.

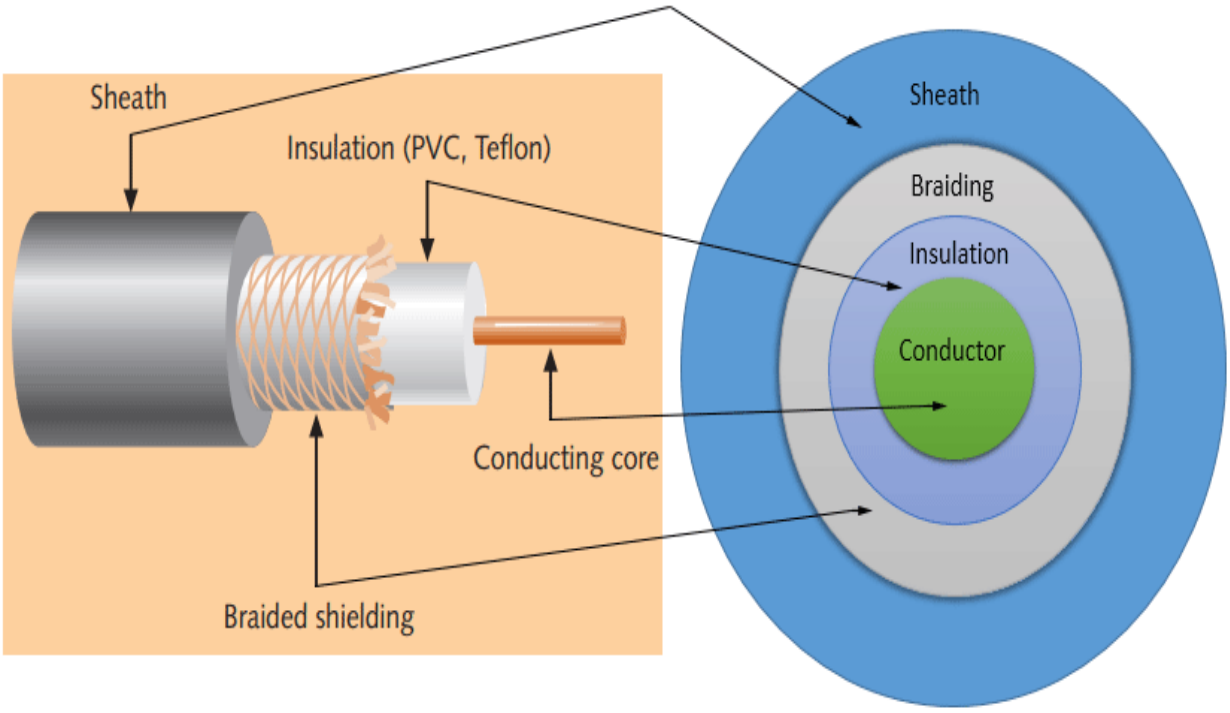
This cable contains a conductor, insulator, braiding, and sheath. The sheath covers the braiding, braiding covers the insulation, and the insulation covers the conductor.

The following image shows these components.

SHEATH

This is the outer layer of the coaxial cable. It protects the cable from physical damage.

BRAIDED SHIELD



This shield protects signals from external interference and noise. This shield is built from the same metal that is used to build the core.

INSULATION

Insulation protects the core. It also keeps the core separate from the braided-shield. Since both the core and the braided-shield use the same metal, without this layer, they will touch each other and create a short-circuit in the wire.

CONDUCTOR

The conductor carries electromagnetic signals. Based on conductor a coaxial cable can be categorized into two types; single-core coaxial cable and multi-core coaxial cable.

A single-core coaxial cable uses a single central metal (usually copper) conductor, while a multi-core coaxial cable uses multiple thin strands of metal wires. The following image shows both types of cable.

The coaxial cables were not primarily developed for the computer network. These cables were developed for general purposes. They were in use even before computer networks came into existence. They are still used even their use in computer networks has been completely discontinued.

At the beginning of computer networking, when there were no dedicated media cables available for computer networks, network administrators began using coaxial cables to build computer networks.

Because of low-cost and long durability, coaxial cables were used in computer networking for nearly two decades (80s and 90s). Coaxial cables are no longer used to build any type of computer network.

TYPES OF COAXIAL CABLES

The common types of coaxial cable include:

- Hard line coaxial cable
- Flexible coaxial cable
- Semi-rigid coaxial cable
- Formable coaxial cable
- Rigid coaxial cable
- Twin axial cable
- Triaxial cable

HARD LINE COAXIAL CABLE

Hard line coaxial cable makes use of a center conductor that is constructed out of materials such as copper, silver, aluminum, or steel and this type of cable is typically larger in diameter than other forms of coaxial cable. These types of cables may be used in high-strength signal transmission. Some forms of hard line make use of pressurized nitrogen as an inhibitor to moisture intrusion as well as to prevent arcing.

FLEXIBLE COAXIAL CABLE

As the name implies, flexible coaxial cable can move and flex as needed to suit the configuration and geometry of the application. A typical design for flexible coaxial cable utilizes a metal inner conductor surrounded by a flexible polymer that functions as the dielectric, with an outer jacket for protection from the environment. When there is a need to increase flexibility, the metal core conductor may be switched to a stranded design from a solid wire, and a polyethylene (PE) dielectric foam may be substituted for the more rigid dielectric material.

Flexible coaxial cable is the most common type of coaxial cable, familiar to anyone who has seen it in use for the connection of home video equipment and televisions.

SEMI-RIGID COAXIAL CABLE

Semi-rigid coaxial cable makes use of a solid copper outer sheath with a dielectric of PTFE. The copper sheath generally provides superior shielding effectiveness and the dielectric properties offer enhanced high frequency performance. By their design, this type of coaxial cable is not intended to be reformed or flexed after the initial forming operation has occurred.

FORMABLE COAXIAL CABLE

An alternative to semi-rigid coaxial cable is formable coaxial cable, also known as conformable coaxial cable. In place of a rigid copper outer sheath, a flexible metal sheath is used, which can be reshaped and formed by hand the meet the desired cable configuration requiring any specialized tools. Formable coax is sometimes used to layout the design for cable placement in prototype applications, and once stabilized, the design is converted to make use of the semi-rigid coaxial cable.

RIGID COAXIAL CABLE

Rigid coaxial cable, sometimes called rigid line, consists of two concentrically mounted copper tubes that are supported at fixed intervals across the length of the cable using PTFE supports or disk insulators. Although it is called a rigid coaxial cable, the term rigid coaxial transmission line may be a more appropriate moniker given that cable is traditionally envisioned as being flexible or bendable. Rigid transmission lines are manufactured and sold in flanged straight sections of a given fixed length. As a result, a set of standard connectors or couplings, such as 45- or 90-degree elbows, are available to join the sections of transmission line together as needed. Specialized braces and springs are used as well to allow for the differential expansion and contraction of the inner and outer copper tubes used in the transmission line run.

TWINAXIAL CABLE

Twinaxial cables (also known as Twin axial or Twinax) have two central conductors contained in the core with a single outer core and dielectric, instead of the traditional one conductor design of most coaxial cable types. Some advantages of twin axial cable are reduced cable loss, greater protection from ground loops and capacitive fields, and a reduction in low-frequency magnetic noise. These cables are best suited for use in low-frequency digital and video applications.

TRIAXIAL CABLE

Triaxial cable, also called triax, are coaxial cables to which an additional copper braid has been added. This braid functions as a shield and is grounded, thus passing any ground loop currents or capacitive field noise away from the inner core conductive elements. Triaxial cable provides increased bandwidth and interference rejection, offers an improvement in signal-to-noise ratio over that of standard coaxial cable, and reduces cable losses and cable loading.

OTHER TYPES OF COAXIAL CABLE

A few other specialized types of coaxial cable include:

a. Coaxial Ribbon Cable Assemblies
b. Micro Coaxial Cable
c. High-frequency Coaxial Cable
d. High-temperature Coaxial Cable
e. Water-cooled Coaxial Cable

SPECIFICATIONS OF COAXIAL CABLES

Coaxial cables have been in use for the last four decades. During these years, based on several factors such as the thickness of the sheath, the metal of the conductor, and the material used in insulation, hundreds of specifications have been created to specify the characteristics of coaxial cables. From these specifications, only a few were used in computer networks. The following table lists them.

TYPES	OHMS	AWG	CONDUCTOR	DESCRIPTION
RG-6	75	18	Solid copper	Used in cable network to provide cable Internet service and cable TV over long distances.
RG-8	50	10	Solid copper	Used in the earliest computer networks. This cable was used as the backbone-cable in the bus topology. In Ethernet standards, this cable is documented as the 10base5 Thicknet cable.
RG-58	50	24	Several thin strands of copper	This cable is thinner, easier to handle and install than the RG-8 cable. This cable was used to connect a system with the backbone-cable. In Ethernet standards, this cable is documented as the 10base2 Thinnet cable.
RG-59	75	20 - 22	Solid copper	Used in cable networks to provide short-distance service.

Coaxial cable uses RG rating to measure the materials used in shielding and conducting cores.

RG stands for the Radio Guide. Coaxial cable mainly uses radio frequencies in transmission.

Impedance is the resistance that controls the signals. It is expressed in the ohms and they are 50, 52, 75, or 93 ohms.

AWG stands for American Wire Gauge. It is used to measure the size of the core. The larger the AWG size, the smaller the diameter of the core wire.

ADVANTAGES OF FIBRE OPTIC CABLE OVER COAXIAL CABLE

- **FIBER OPTICS ARE SIGNIFICANTLY FASTER THAN COAXIAL CABLES**

Although optical fibers are hair-thin, they have the capacity for greater bandwidth than traditional cables. Fiber technology has transformed the way we transmit data, video and voice.

- **FIBER OPTICS ARE ECO-FRIENDLY THAN COAXIAL CABLES**

The copper cables stored in data centers produce a significant amount of excess heat. This requires cooling systems to work harder to keep the center at an appropriate temperature.

Fiber-optic technology, on the other hand, does not generate excess heat. Therefore, not as much energy is required to cool down the data centers.

Additionally, fiber-optic cables require less insulation and jacketing than copper cables. Heavy metals are often used in wire insulation and jacketing, and it's better for the environment to avoid using these materials when possible.

- **FIBER OPTICS IS THE TECHNOLOGY OF THE FUTURE**

Fiber-optic Internet simply provides more bandwidth than cable. With more bandwidth, fiber optics more easily allow for data-heavy Internet tasks that you regularly perform – such as online gaming, streaming TV shows and movies, video chatting and more.

As more and more devices in the home require an Internet connection, it is possible that coaxial cables will not be able to support households' Internet demands. Fiber-optic Internet will be able to support more bandwidth-intensive activities.

Finally, fiber optics is typically upgraded through advancements to the electronic light pulse technology, not by replacing the cable equipment. For this reason, fiber is considered "future proof" – the technology can easily evolve.

❖ FIBER OPTICS OFFER MORE SECURE COMMUNICATION THAN COAXIAL CABLES

One benefit of fiber-optic technology is increased security. It is more difficult to tap fiber-optic cables than traditional copper cables. It would be hard to tap fiber-optic cables without also disrupting the system.

Additionally, the signals of fiber-optic cables are considered dielectric and do not transmit electricity. This makes data interception very difficult compared to the electromagnetic signals of coaxial cables.

FIBER OPTIC CABLE

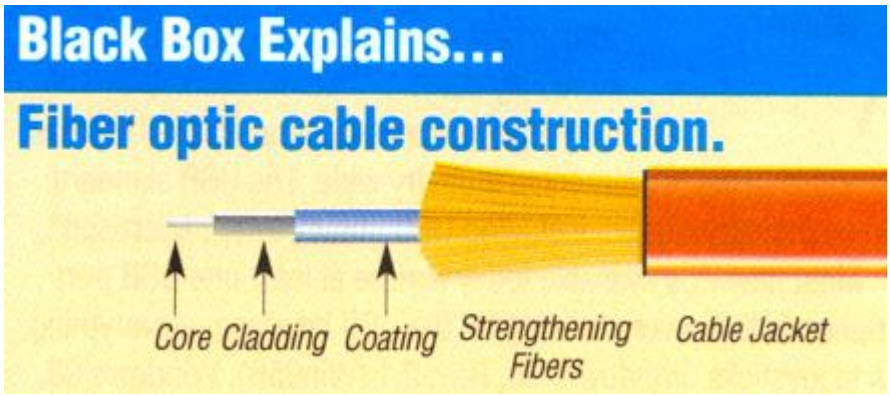
This cable consists of core, cladding, buffer, and jacket. The core is made from the thin strands of glass or plastic that can carry data over the long distance. The core is wrapped in the cladding; the cladding is wrapped in the buffer, and the buffer is wrapped in the jacket.

Core carries the data signals in the form of the light.

Cladding reflects light back to the core.

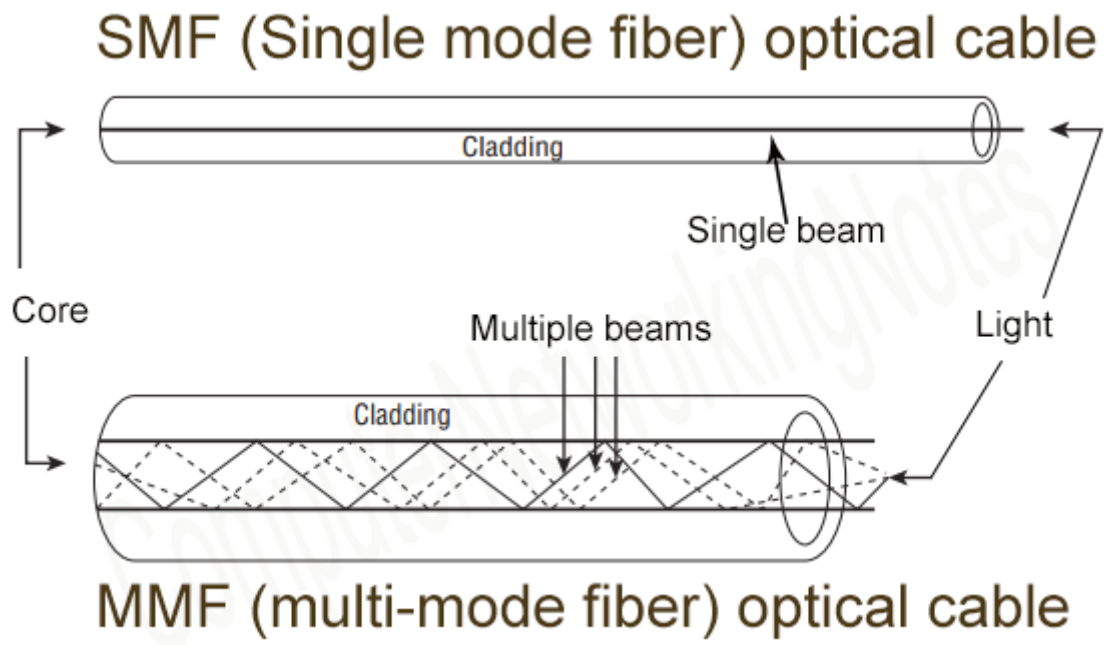
Buffer protects the light from leaking.

The jacket protects the cable from physical damage.



Fiber optic cable is completely immune to EMI (Electromagnetic Influence) and RFI(Radio Frequency Interference). This cable can transmit data over a long distance at the highest speed. It can transmit data up to 40 kilometers at the speed of 100Gbps.

Fiber optic uses light to send data. It reflects light from one endpoint to another. Based on how many beams of light are transmitted at a given time, there are two types of fiber optical cable; SMF and MMF.



TYPES OF FIBRE OPTICS CABLES

There are three types of fiber optic cable commonly used:-

- Single-Mode Fiber Optic Cable
- Multi-Mode Fibre Optic Cable and
- Plastic Optical Fiber (POF).

SMF (SINGLE-MODE FIBER) OPTICAL CABLE

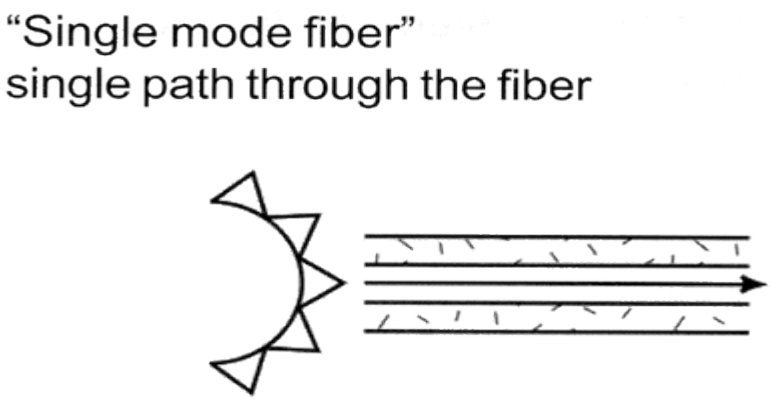
Single Mode cable is a single stand of glass fiber with a diameter of 8.3 to 10 microns that has one mode of transmission. Single Mode Fiber with a relatively narrow diameter, through which only one mode will propagate typically 1310 or 1550nano-meter wavelength of light. Carries higher bandwidth than multimode fiber, but requires a light source with a narrow spectral width.

Synonyms mono-mode optical fiber, single-mode fiber, single-mode optical waveguide, uni-mode fiber.

Single Modem fiber is used in many applications where data is sent at multi-frequency (WDM Wave-Division-Multiplexing) so only one cable is needed - (single-mode on one single fiber)

Single-mode fiber gives you a higher transmission rate and up to 50 times more distance than multimode, but it also costs more. Single-mode fiber has a much smaller core than multimode. The small core and single light-wave virtually eliminate any distortion that could result from overlapping light pulses, providing the least signal attenuation and the highest transmission speeds of any fiber cable type.

Single-mode optical fiber is an optical fiber in which only the lowest order bound mode can propagate at the wavelength of interest typically 1300 to 1320nm.

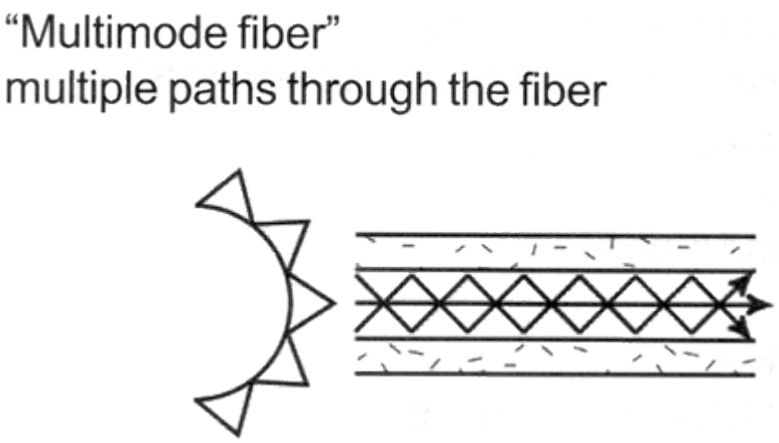


MMF (MULTI-MODE FIBER) OPTICAL CABLE

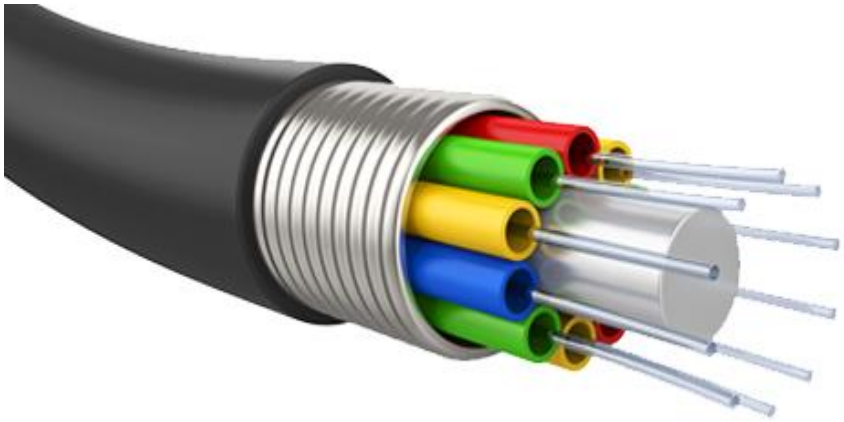
Multi-Mode cable has a little bit bigger diameter, with a common diameter in the 50-to-100 micron range for the light to carry component. Most applications in which Multi-mode fiber is used, 2 fibers are used (WDM is not normally used on multi-mode fiber).

POF is a newer plastic-based cable which promises performance similar to glass cable on very short runs, but at a lower cost.

Multimode fiber gives you high bandwidth at high speeds (10 to 100MBS - Gigabit to 275m to 2km) over medium distances. Light waves are dispersed into numerous paths, or modes, as they travel through the cable's core typically 850 or 1300nm. Typical multimode fiber core diameters are 50, 62.5, and 100 micrometers. However, multiple paths of light can cause signal distortion at the receiving end, resulting in an unclear and incomplete data transmission so designers now call for single mode fiber in new applications using Gigabit and beyond.



ADVANTAGES OF FIBRE OPTIC CABLE OVER COPPER CABLING



1. **GREATER BANDWIDTH**

Copper cables were originally designed for voice transmission and have a limited bandwidth. Fiber optic cables provide more bandwidth for carrying more data than copper cables of the same diameter. Within the fiber cable family, single mode fiber delivers up to twice the throughput of multimode fiber.

2. **FASTER SPEEDS**

Fiber optic cables have a core that carries light to transmit data. This allows fiber optic cables to carry signals at speeds that are only about 31 percent slower than the speed of light—faster than Cat5 or Cat6 copper cables. There is also less signal degradation with fiber cables.

3. **LONGER DISTANCES**

Fiber optic cables can carry signals much farther than the typical 328-foot limitation for copper cables. For example, some 10 Gbps single mode fiber cables can carry signals almost 25 miles. The actual distance depends on the type of cable, the wavelength and the network.

4. **BETTER RELIABILITY**

Fiber is immune to temperature changes, severe weather and moisture, all of which can hamper the connectivity of copper cable. Plus, fiber does not carry electric current, so it’s not bothered by electromagnetic interference (EMI) that can interrupt data transmission. It also does not present a fire hazard like old or worn copper cables can.

5. **THINNER AND STURDIER**

Compared to copper cables, fiber optic cables are thinner and lighter in weight. Fiber can withstand more pull pressure than copper and is less prone to damage and breakage.

6. MORE FLEXIBILITY FOR THE FUTURE

Media converters make it possible to incorporate fiber into existing networks. The converters extend UTP Ethernet connections over fiber optic cable. Modular patch panel solutions integrate equipment with 10 Gb, 40 Gb and 100/120 Gb speeds to meet current needs and provide flexibility for future needs. The panels in these solutions accommodate a variety of cassettes for different types of fiber patch cables.

7. LOWER TOTAL COST OF OWNERSHIP

Although some fiber optic cables may have a higher initial cost than copper, the durability and reliability of fiber can make the total cost of ownership (TCO) lower. And, costs continue to decrease for fiber optic cables and related components as technology advances.

TWISTED-PAIR CABLES

The twisted-pair cable was primarily developed for computer networks. This cable is also known as Ethernet cable. Almost all modern LAN computer networks use this cable.

This cable consists of color-coded pairs of insulated copper wires. Every two wires are twisted around each other to form pair. Usually, there are four pairs. Each pair has one solid color and one stripped color wire. Solid colors are blue, brown, green and orange. In stripped color, the solid color is mixed with the white color.

Based on how pairs are stripped in the plastic sheath, there are two types of twisted-pair cable namely: -

- UTP (Unshielded twisted-pair) cable and
- STP (Shielded twisted-pair) cable.

UTP (UNSHIELDED TWISTED-PAIR CABLE): - In the UTP (Unshielded twisted-pair) cable, all pairs are wrapped in a single plastic sheath.

Unshielded twisted pair (UTP) cables are widely used in the computer and telecommunications industry as Ethernet cables and telephone wires.

In an UTP cable, conductors which form a single circuit are twisted around each other in order to cancel out electromagnetic interference (EMI) from external sources. Unshielded means no additional shielding like meshes or aluminum foil, which add bulk, are used. UTP cables are often groups of twisted pairs grouped together with color coded insulators, the number of which depends on the purpose.

An UTP cable is made up of a bundle of twisted pairs. The twisted pairs are small 22- or 24-American Wire Gauge (AWG) sized wires twisted around each other.

The wires are typically made of copper with polyethylene (PE) or FEP insulation which is color coded depending on the application of the cable being made.

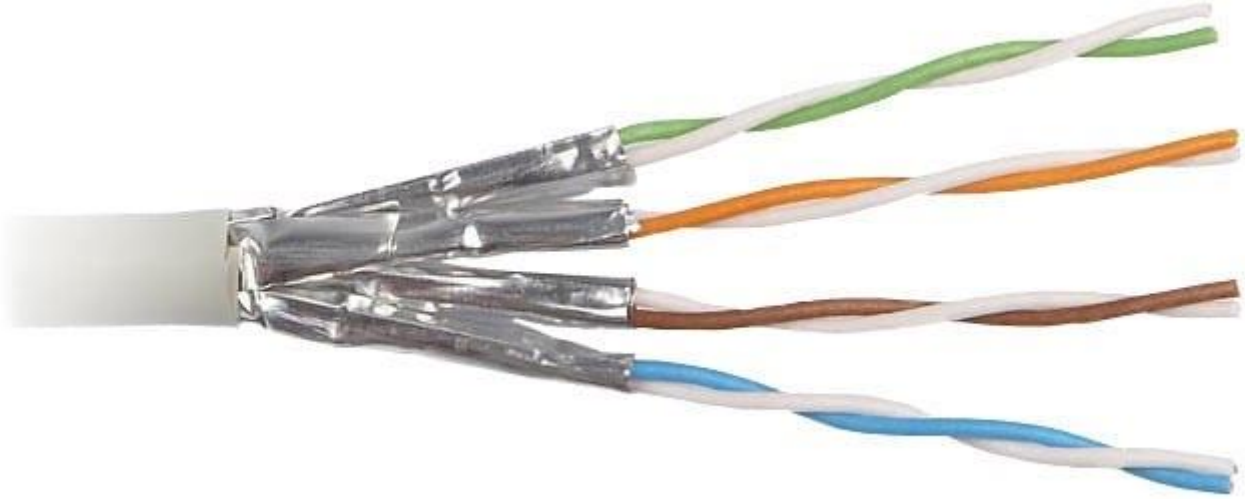
For instance, AT&T pioneered the 25-pair color code UTP cable for indoor telephone applications with color-pairs like white-blue, blue-white, white-orange, orange-white and others.

The bundle is often covered with a PE jacket typically colored grey. The two wires carry equal yet opposite signals and the destination of the signal detects the difference between the two.

They are typically used in computer networking such as Ethernet for short-to-medium distances because of their relatively cheap price compared to optical fiber and coaxial cables.

Unshielded Twisted Pair (UTP) cable is most certainly by far the most popular cable around the world. UTP cable is used not only for networking but also for the traditional telephone (UTP-Cat 1). There are seven different types of UTP categories and, depending on what you want to achieve, you would need the appropriate type of cable. UTP-CAT5e is the most popular UTP cable which came to replace the old coaxial cable that was not able to keep up with the constant growing need for faster and more reliable networks.

STP (SHIELDED TWISTED-PAIR CABLE): - Is twisted-pair cabling with additional shielding to reduce crosstalk and other forms of electromagnetic interference (EMI).



Shielded Twisted-pair Cable

The outer insulating jacket contains an inner braided copper mesh to shield the pairs of twisted cables, which themselves are wrapped in foil.

Shielded twisted-pair (STP) cabling is more expensive than unshielded twisted-pair (UTP) cabling. It has an impedance of 150 ohms, has a maximum length of 90 meters, and is used primarily in networking environments with a high amount of EMI due to motors, air conditioners, power lines, or other noisy electrical components. STP cabling is the default type of cabling for IBM Token Ring networks.

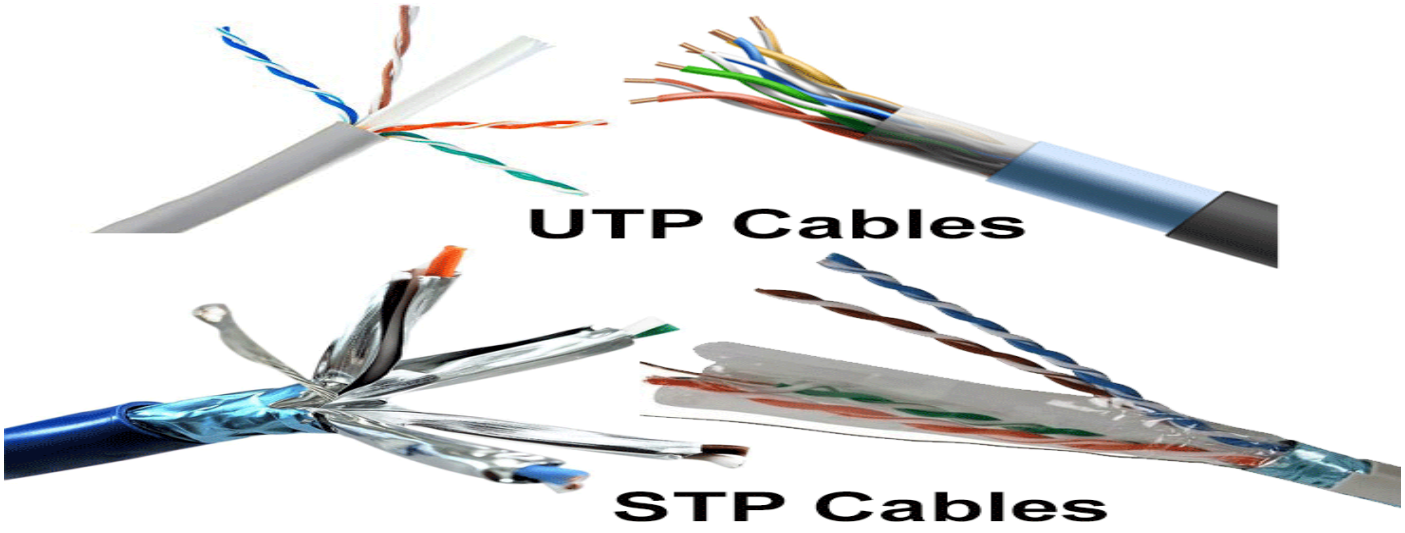
DIFFERENCE BETWEEN UNSHIELDED TWISTED PAIR (UTP) AND SHIELDED TWISTED PAIR (STP) CABLES:

S.NO	UTP	STP
1.	UTP stands for Unshielded twisted pair.	STP stands for Shielded twisted pair.
2.	In UTP grounding cable is not necessary.	While in STP grounding cable is required.
3.	Data rate in UTP is slow compared to STP.	Data rate in STP is high.
4.	The cost of UTP is less.	While STP is costlier than UTP.
5.	In UTP much more maintenance are not needed.	While in STP much more maintenance are needed.
6.	In UTP noise is high compared to STP.	While in STP noise is less.
7.	In UTP the generation of crosstalk is also high compared to STP.	While in STP generation of crosstalk is also less.
8.	In UTP, attenuation is high in comparison to STP.	While in STP attenuation is low.

SIMILARITIES BETWEEN UTP AND STP

- Both STP and UTP can transmit data at 10Mbps, 100Mbps, 1Gbps, and 10Gbps.
- Both cables use the same RJ-45 (registered jack) modular connectors.
- The maximum segment length for both cables is 100 meters or 328 feet.
- Both cables can accommodate a maximum of 1024 nodes in each segment.

The following image shows both types of twisted-pair cable.



The Telecommunications Industry Association (TIA) / Electronic Industries Alliance (EIA) specifies standards for the twisted-pair cable. First standards were released in 1991, known as TIA/EIA 568. Since then, these standards have been continually revised to cover the latest technologies and developments of the transmission media.

The TIA/EIA 568 divides the twisted-pair cable into several categories. The following table lists the most common and popular categories of the twisted-pair cable.

CATEGORY /NAME OF THE CABLE	MAXIMUM SUPPORTED SPEED	BANDWIDTH / SUPPORT SIGNAL RATE	ETHERNET STANDARD	DESCRIPTION
Cat 1	1Mbps	1MHz	Not used for data	This cable contains only two pairs (4 wires). This cable was used in the telephone network for voice transmission.
Cat 2	4Mbps	10MHz	Token Ring	This cable and all further cables have a minimum of 8 wires (4 pairs). This cable was used in the token-ring network.
Cat 3	10Mbps	16MHz	10BASE-T Ethernet	This is the first Ethernet cable that was used in LAN networks.
Cat 4	20Mbps	20MHz	Token Ring	This cable was used in advanced Token-ring networks.
Cat 5	100Mbps	100MHz	100BASE-T Ethernet	This cable was used in advanced (fast) LAN networks.
Cat 5e	1000Mbps	100MHz	1000BASE-T Ethernet	This cable/category is the minimum requirement for all modern LAN networks.
Cat 6	10Gbps	250MHz	10GBASE-T Ethernet	This cable uses a plastic core to prevent cross-talk between twisted-pair. It also uses a fire-resistant plastic sheath.
Cat 6a	10Gbps	500MHz	10GBASE-T Ethernet	This cable reduces attenuation and cross-talk. This cable also potentially removes the length limit. This is the recommended cable for all modern Ethernet LAN networks.
Cat 7	10Gbps	600MHz	Not drafted yet	This cable sets a base for further development. This cable uses multiple twisted-pairs and shields each pair by its own plastic sheath.

Cat 1, 2, 3, 4, 5 are outdated and not used in any modern LAN network.

Cat 7 is still a new technology and not commonly used.

Cat 5e, 6, 6a are the commonly used twisted-pair cables.

WHAT IS IEEE?

IEEE, or the Institute of Electrical and Electronics Engineers, is an organization composed of engineers that issues and manages standards for electrical and electronic devices. This includes networking devices, network interfaces, cablings and connectors.

ETHERNET

Ethernet, pronounced "E-thernet" (with a long "e"), is the standard way to connect computers on a network over a wired connection. It provides a simple interface and for connecting multiple devices, such computers, routers, and switches. With a single router and a few Ethernet cables, you can create a LAN, which allows all connected devices to communicate with each other.
A standard Ethernet cable is slightly thicker than a phone cable and has an RJ45 connector on each end. Ethernet ports look similar to telephone jacks, but are slightly wider. You can plug or unplug devices on an Ethernet network while they are powered on without harming them.
Like USB, Ethernet has multiple standards that all use the same interface. These include:

- 10BASE-T - supports up to 10 Mbps
- 100BASE-T - supports up to 100 Mbps
- 1000BASE-T (also called "Gigabit Ethernet") - supports up to 1,000 Mbps

Most Ethernet devices are backwards compatible with lower-speed Ethernet cables and devices. However, the connection will only be as fast as the lowest common denominator. For example, if you connect a computer with a 10BASE-T NIC to a 100BASE-T network, the computer will only be able to send and receive data at 10 Mbps. If you have a Gigabit Ethernet router and connect devices to it using 100BASE-T cables, the maximum data transfer rate will be 100 Mbps.
While Ethernet is still the standard for wired networking, it has been replaced in many areas by wireless networks. Wi-Fi allows you to connect your laptop or smartphone to a network without being tethered to the wall by a cable. The 802.11ac Wi-Fi standard even provides faster maximum data transfer rates than Gigabit Ethernet. Still, wired connections are less prone to interference and are more secure than wireless ones, which is why many businesses and organizations still use Ethernet.

NOTE: Ethernet is also known by its technical name, "IEEE 802.3."

Internet is a communication protocol for worldwide network (WAN = Wide Area Network). Devices are managed through this network on the basis of IP addresses.

Ethernet is a communication protocol for Local Area Network (LAN) using same media interfaces (mainly RJ45 or fiber). LAN are independent networks but may be linked within a WAN through Internet devices such as Routers.

ELECTROMAGNETIC INTERFERENCE (EMI)

EMI, Electromagnetic Interference, is electrical noise induced in cabling by the presence of nearby electrical equipment such as motors, air conditioners, fluorescent lights, and power lines.

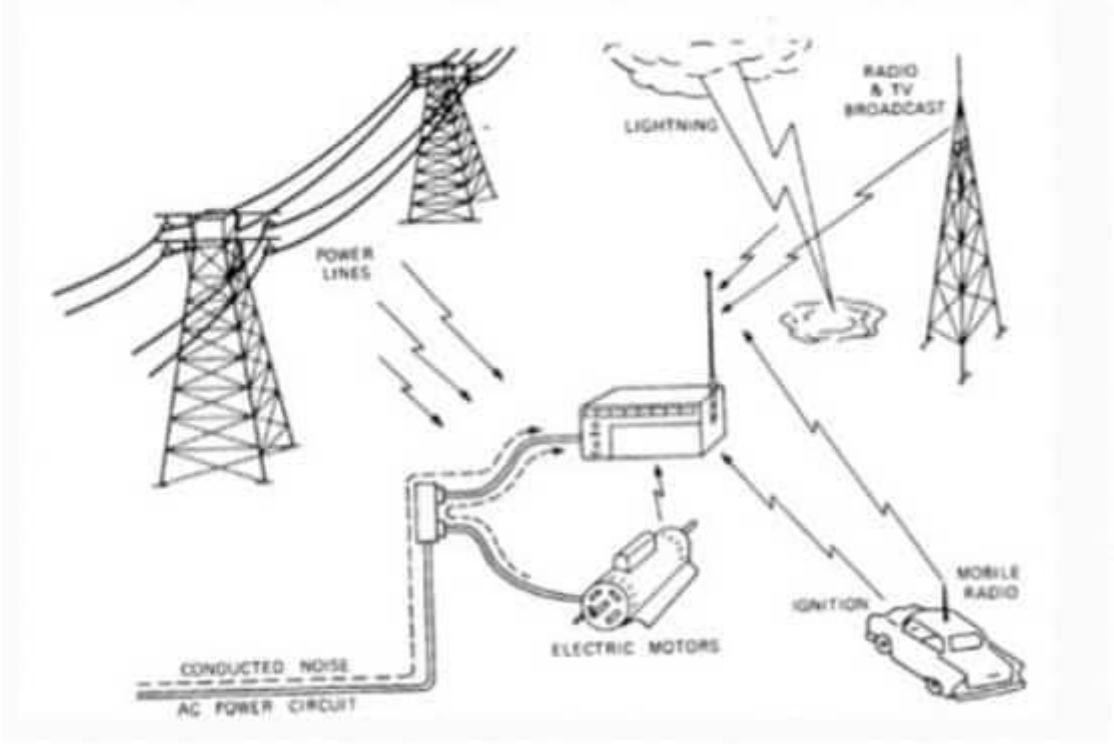
WHAT IS EMI (ELECTROMAGNETIC INTERFERENCE)?

EMI is the electrical noise induced in cabling by the presence of nearby electrical equipment such as motors, air conditioners, fluorescent lights, and power lines. Electromagnetic interference (EMI) can interfere with the transmission of signals.

EMI is only a problem with copper cabling. It's caused when the changing electromagnetic fields generated by one cable induce extraneous currents or interference in adjacent or nearby cables. EMI in copper cabling can be reduced to acceptable levels by

- Avoiding bunching of unshielded cabling
- Keeping all cabling away from power cords and transformers
- Using shielded twisted-pair (STP) cabling instead of unshielded twisted-pair (UTP) cabling
- Enclosing cabling in external mesh or wire shielding
- Properly grounding electrical equipment and external shielding
- Taking care not to excessively untwist the terminating ends of twisted-pair cabling

Electromagnetic interference (EMI)



Electromagnetic Interference examples

EMI can be a greater concern in heavy industrial settings where high voltages and equipment, such as motors and generators, produce high levels of electrical noise. Using coaxial cabling in these settings affords greater resistance to the effects of EMI than using twisted-pair cabling. Fiber-optic cabling is an even better solution in heavy industrial settings because it is wholly resistant to EMI. (Changing electromagnetic fields have no effect on the light waves traveling along a glass fiber.)

HOW TO PREVENT ELECTROMAGNETIC INTERFERENCE?

Because anything that carries rapidly changing electrical currents gives off electromagnetic emissions, it is quite common for one object's emissions to "interfere" with another's. EMI compromises the performance of electrical equipment by obstructing and degrading data; sometimes even losing data completely.

EMI regulations help keep the multitude of electronic devices functioning properly. Without these regulations, our electronic devices would suffer a significant degradation of performance and data loss.

Some basic options for preventing EMI include:

- Keeping electronic devices away from heavy machinery, motors or generators.
- Using shielded cables.

- Using EMI filters
- Using a snubber network between two contacts under 2 A

CAN ELECTROMAGNETIC INTERFERENCE (EMI) BE MEASURED?

We can detect Electromagnetic Interference and measure Electromagnetic Fields. Check the example below:

Some basic options for preventing EMI include:

- Keeping electronic devices away from heavy machinery, motors or generators.
- Using shielded cables.
- Using EMI filters
- Using a snubber network between two contacts under 2 A

SUMMARY ON INTRODUCTION TO NETWORK CABLES

Network cables transfer data between computers and devices

Even though there have been advances in wireless technologies, many computer networks in the 21st century rely on cables as the physical medium that devices use to transfer data. Several standard types of network cables exist, each designed for specific purposes.

COAXIAL CABLES

Invented in the 1880s, coaxial cable (also called coax) was best known as the kind of cable that connected television sets to home antennas. Coaxial cable is also a standard for 10 Mbps Ethernet cables.

When 10 Mbps Ethernet was most popular, during the 1980s and early 1990s, networks typically used one of two kinds of coax cable — thinnet (10BASE2 standard) or thicknet (10BASE5). These cables consist of an inner copper wire of varying thickness surrounded by insulation and another shielding. Their stiffness caused network administrators difficulty when installing and maintaining thinnet and thicknet.

TWISTED PAIR CABLES

Twisted pair emerged during the 1990s as the leading cabling standard for Ethernet, starting with 10 Mbps (10BASE-T, also known as Category 3 or Cat3), later followed by improved versions for 100 Mbps (100BASE-TX, Cat5, and Cat5e) and successively higher speeds up to 10 Gbps (10GBASE-T). Ethernet twisted pair cables contain up to eight wires wound together in pairs to minimize electromagnetic interference.

Two primary types of twisted pair cable industry standards have been defined: unshielded twisted pair (UTP) and shielded twisted pair (STP). Modern Ethernet cables use UTP wiring

due to its lower cost, while STP cabling can be found in other types of networks such as Fiber Distributed Data Interface (FDDI).

FIBER OPTICS

Instead of insulated metal wires transmitting electrical signals, fiber optic network cables use strands of glass and pulses of light. These network cables are bendable despite being made of glass. They have proven especially useful in wide area network (WAN) installations where long-distance underground or outdoor cable runs are required and also in office buildings where a high volume of communication traffic is common.

Two primary types of fiber optic cable industry standards are defined—single-mode (100BaseBX standard) and multimode (100BaseSX standard). Long-distance telecommunications networks commonly use single-mode for its relatively higher bandwidth capacity, while local networks typically use multimode due to its lower cost.

USB CABLES

Most Universal Serial Bus (USB) cables connect a computer with a peripheral device (such as a keyboard or mouse) rather than to another computer. However, special network adapters (sometimes called dongles) connect an Ethernet cable to a USB port indirectly. USB cables feature twisted-pair wiring.

Everything You Need to Know About USB Ports and Cables

SERIAL AND PARALLEL CABLES

Because many PCs in the 1980s and early 1990s lacked Ethernet capability, and USB had not been developed yet, serial and parallel interfaces (now obsolete on modern computers) were sometimes used for PC-to-PC networking. So-called null modem cables, for example, connected the serial ports of two PCs and enabled data transfers at speeds between 0.115 and 0.45 Mbps.

CROSSOVER CABLES

Null modem cables are one example of the category of crossover cables. A crossover cable joins two network devices of the same type, such as two PCs or two network switches. The use of Ethernet crossover cables was common on older home networks years ago when connecting two PCs directly together.

Externally, Ethernet crossover cables appear identical to ordinary cables (sometimes called straight-through), the only visible difference being the order of the color-coded wires

appearing on the cable's end connector. Manufacturers typically applied special distinguishing marks to their crossover cables for this reason. Nowadays, though, most home networks utilize routers that have built-in crossover capability, eliminating the need for these special cables.

OTHER TYPES OF NETWORK CABLES

Some networking professionals use the term patch cable to refer to any kind of straight-through network cable used for a temporary purpose. Coax, twisted pair and fiber optic types of patch cables exist. These cables share the same physical characteristics as other types of network cables except that patch cables tend to be a shorter length.

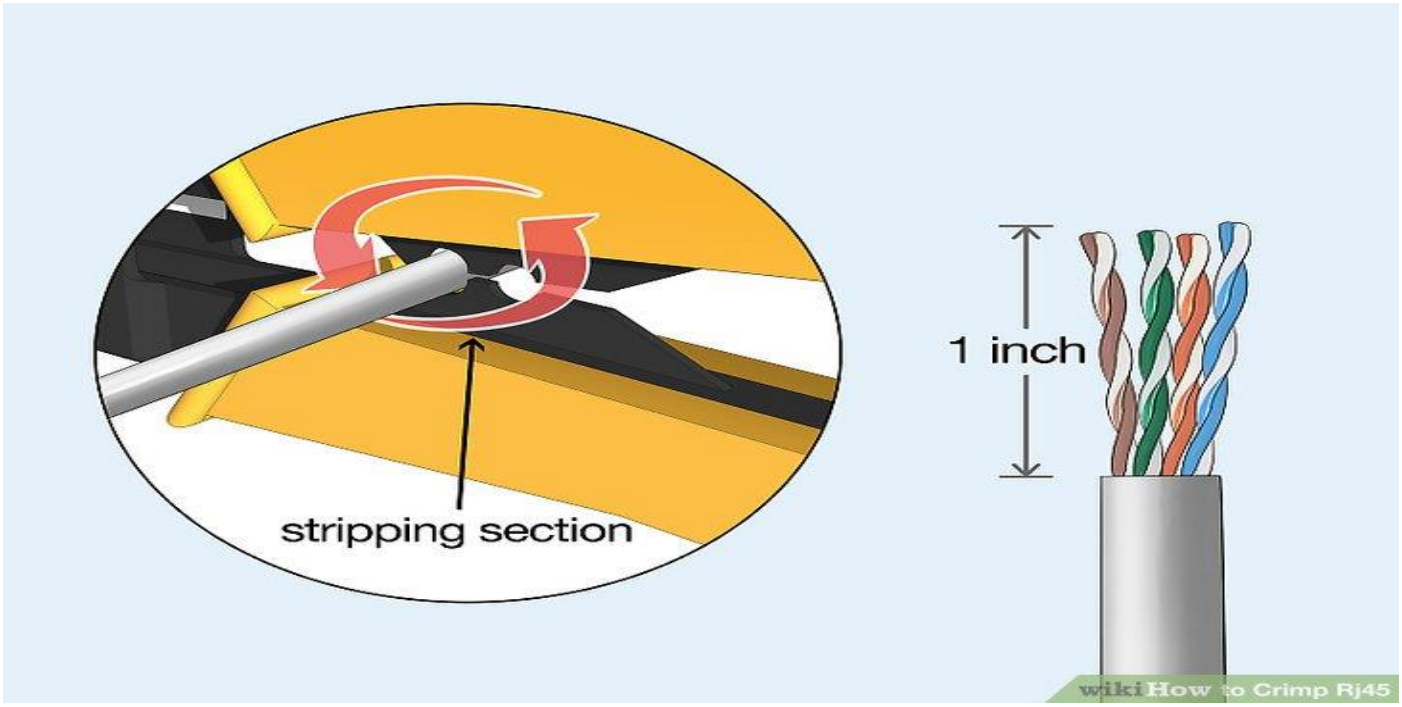
Powerline network systems utilize a home's standard electrical wiring for data communication using special adapters plugged into wall outlets.

HOW TO CRIMP RJ45 TO CABLE WITH OR WITHOUT CRIMPING TOOL

You can quickly and easily crimp an RJ-45 to a cable with or without a crimping tool. If you have a crimping tool, strip away a portion of the sheath, untangle and arrange the wires in the correct order, fit them into the connector, and use the crimping part of your tool to squeeze the small pins into the wires and secure the connector. If you don't have a crimping tool, no problem! Use a pair of scissors or a utility knife to cut away a section of the sheathing at the end of the cable, untwist and arrange the small cables in the right order, put them into the RJ-45 connector, and use a small, flathead screwdriver to press down each of the pins.

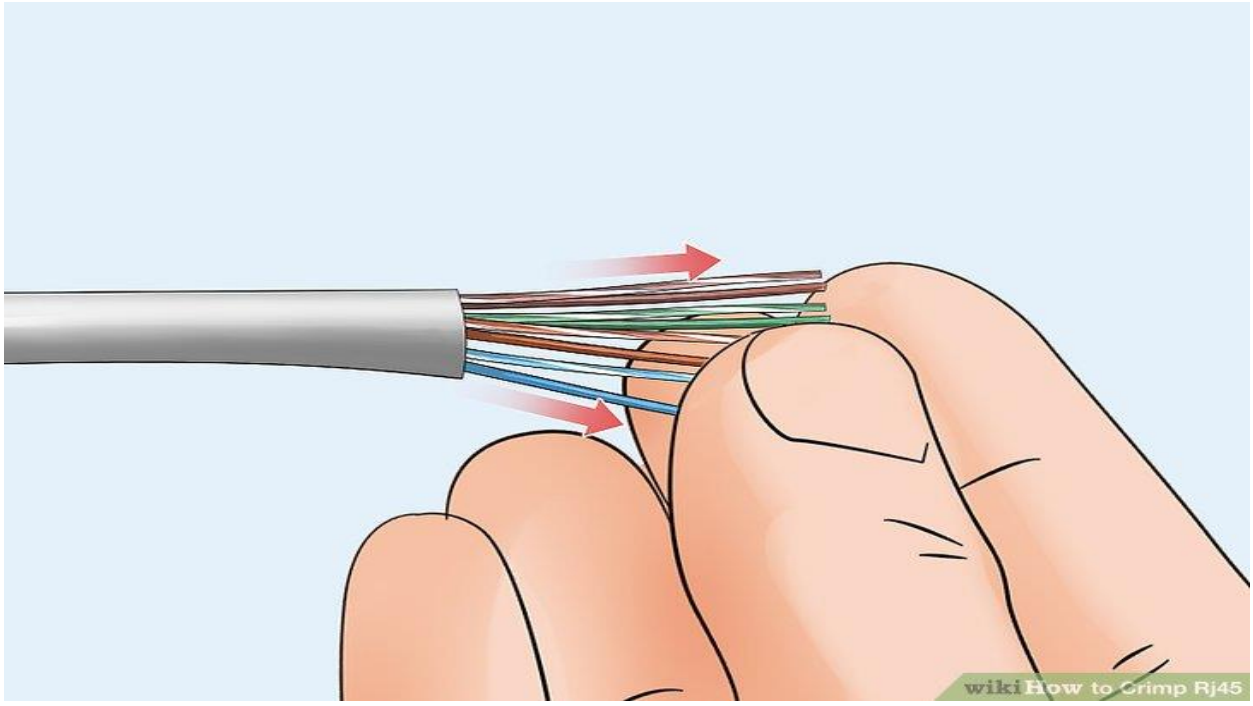
Method1

USING A CRIMPING TOOL



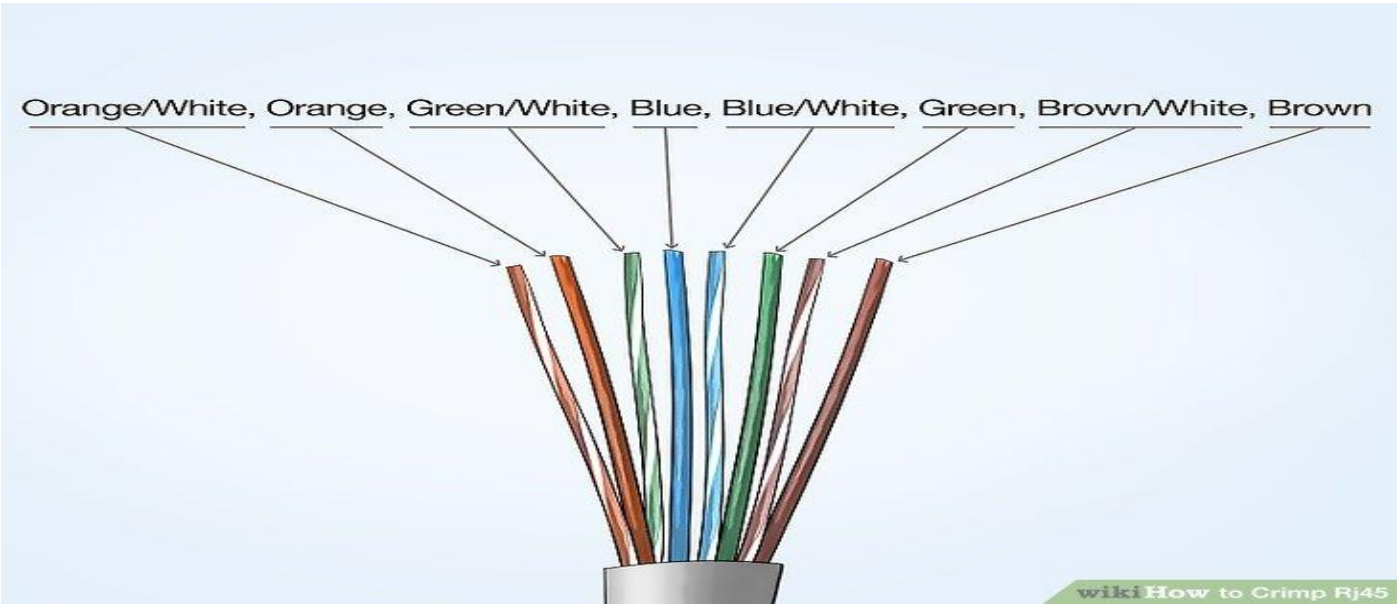
1. Strip the cable back 1 inch (25 mm) from the end. Insert the cable into the stripper section of the tool and squeeze it tight. Then, rotate the crimping tool around the cable in a smooth and even motion to create a clean cut. Keep the tool clamped and pull away towards the end of the wire to remove the sheathing.

- The stripping section is a round hole near the handle of the tool.
- The sheathing should come off cleanly, leaving the wires exposed.



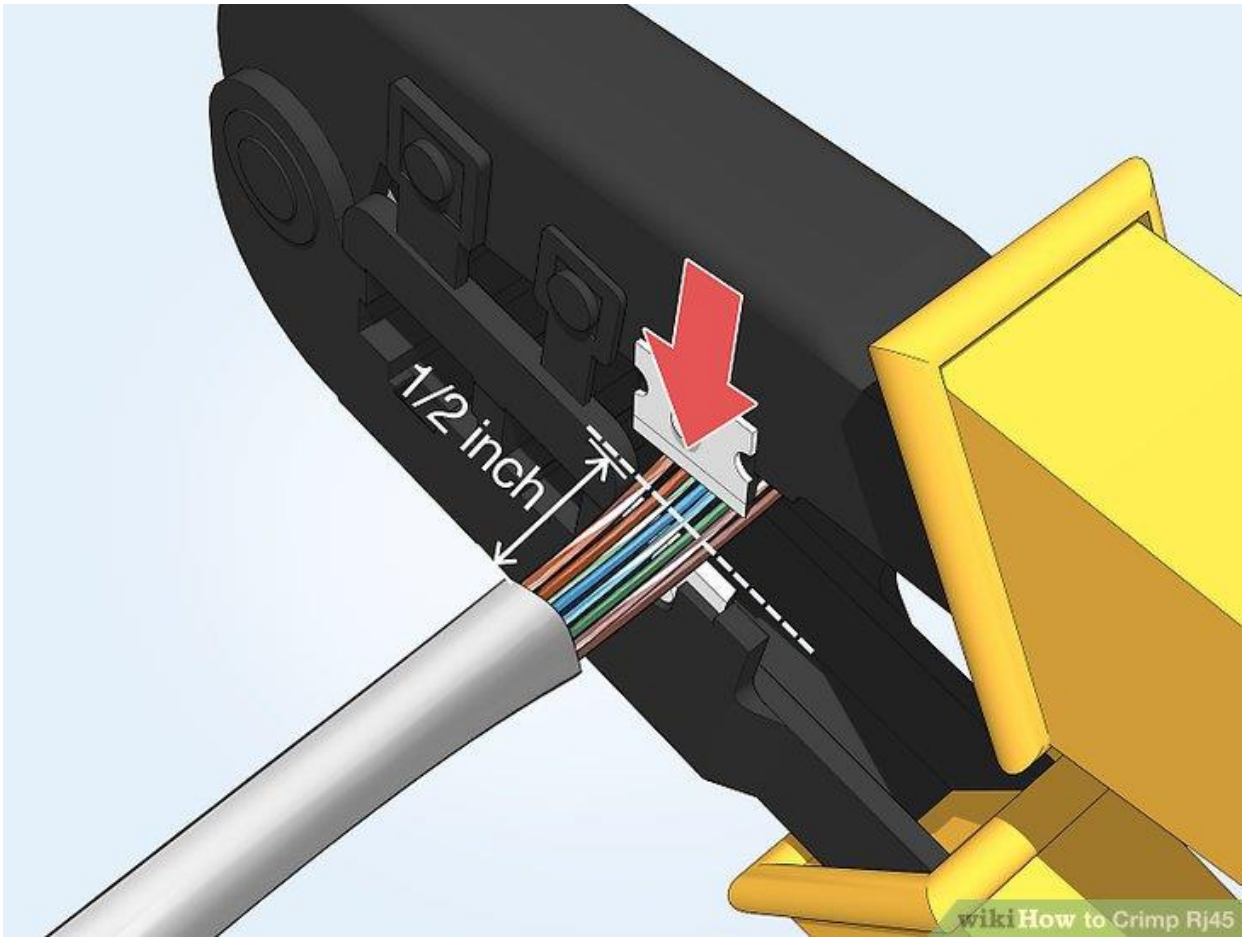
2 Untwist and straighten the wires inside of the cable. Inside of the cable you'll see a bunch of smaller wires twisted together. Separate the twisted wires and straighten them out so they're easier to sort into the right order.

- Cut off the small plastic wire separator or core so it's out of the way.
- Don't cut off or remove any of the wires or you won't be able to crimp them into the connector.



3. Arrange the wires into the right order. Use your fingers to put the wires in the correct order so they can be properly crimped. The proper sequence is as follows from left to right: Orange/White, Orange, Green/White, Blue, Blue/White, Green, Brown/White, Brown.[3]

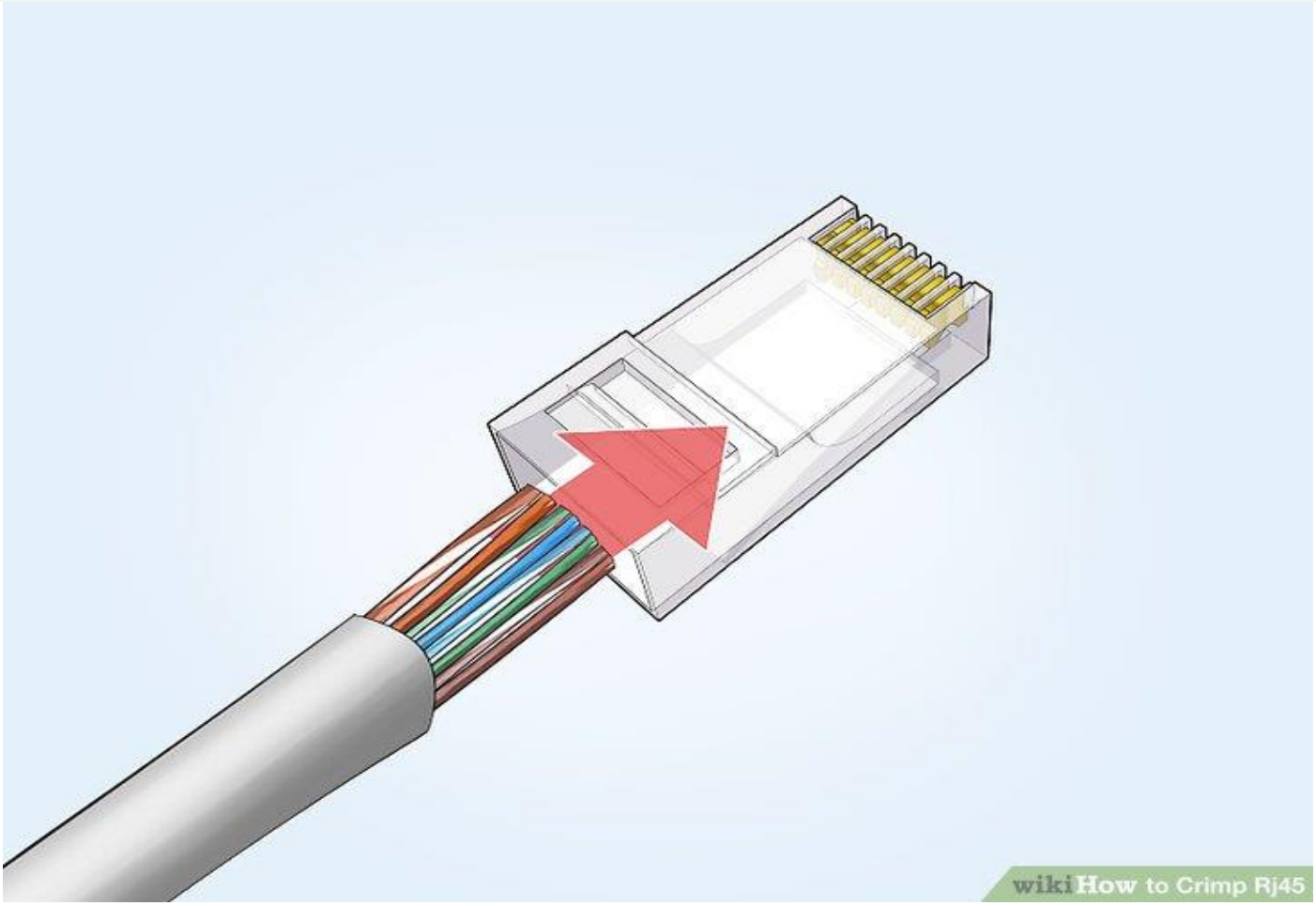
- There are 8 wires in total that need to be arranged in the right sequence.
- Note that the wires labeled Orange/White or Brown/White indicate the small wires that have 2 colors.



4 Cut the wires into an even line ½ inch (13 mm) from sheathing. Hold the wires with your thumb and index finger to keep them in order. Then, use the cutting section of the crimping tool to cut them into an even line.[4]

- The cutting section of the tool will resemble wire cutters.
- The wires must be in an even line to be crimped into the RJ-45 connector properly. If you cut them in an uneven line, move further down the wires and cut them again.

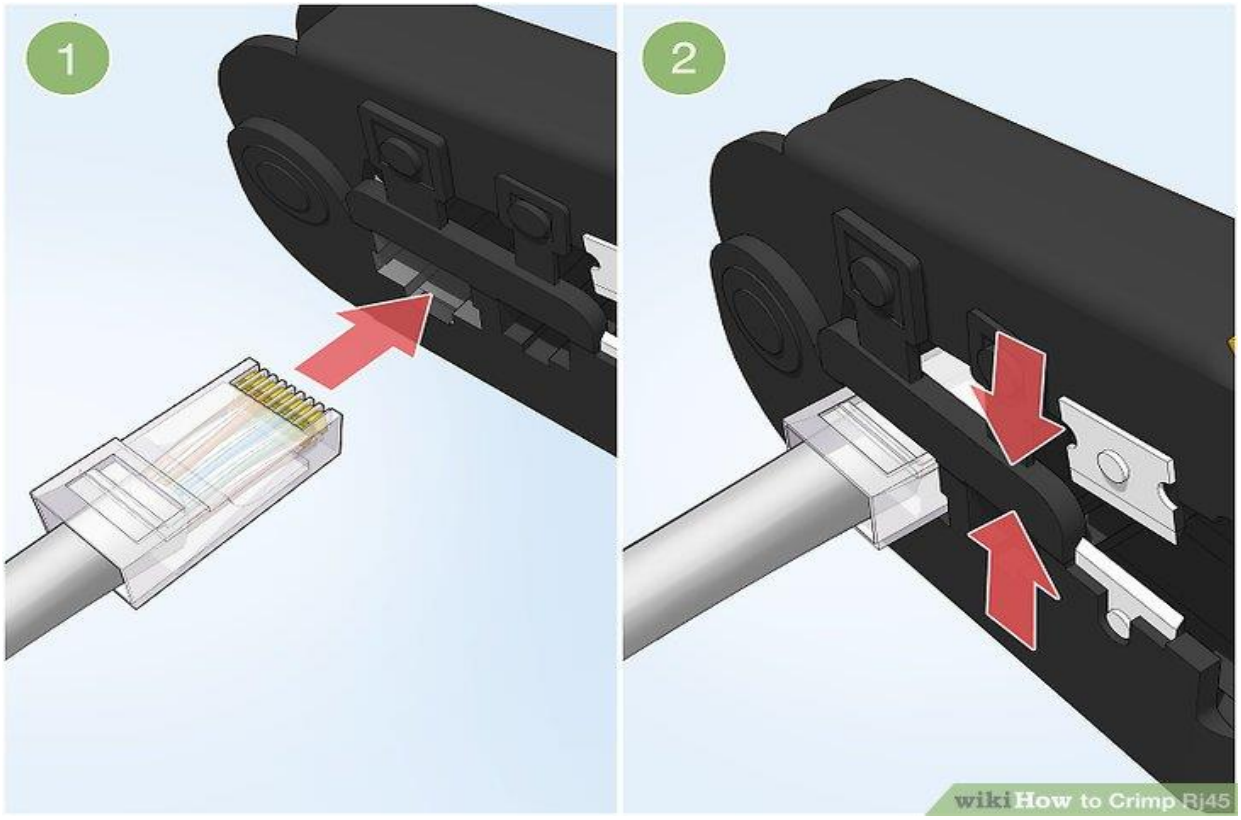
Tip: If your tool doesn’t have a cutting section, use a pair of wire cutters or scissors to cut the small wires.



5. Insert the wires into the RJ-45 connector. Hold the RJ-45 connector so the clip is on the underside and the small metal pins are facing up. Insert the cable into the connector so that each of the small wires fits into the small grooves in the connector.

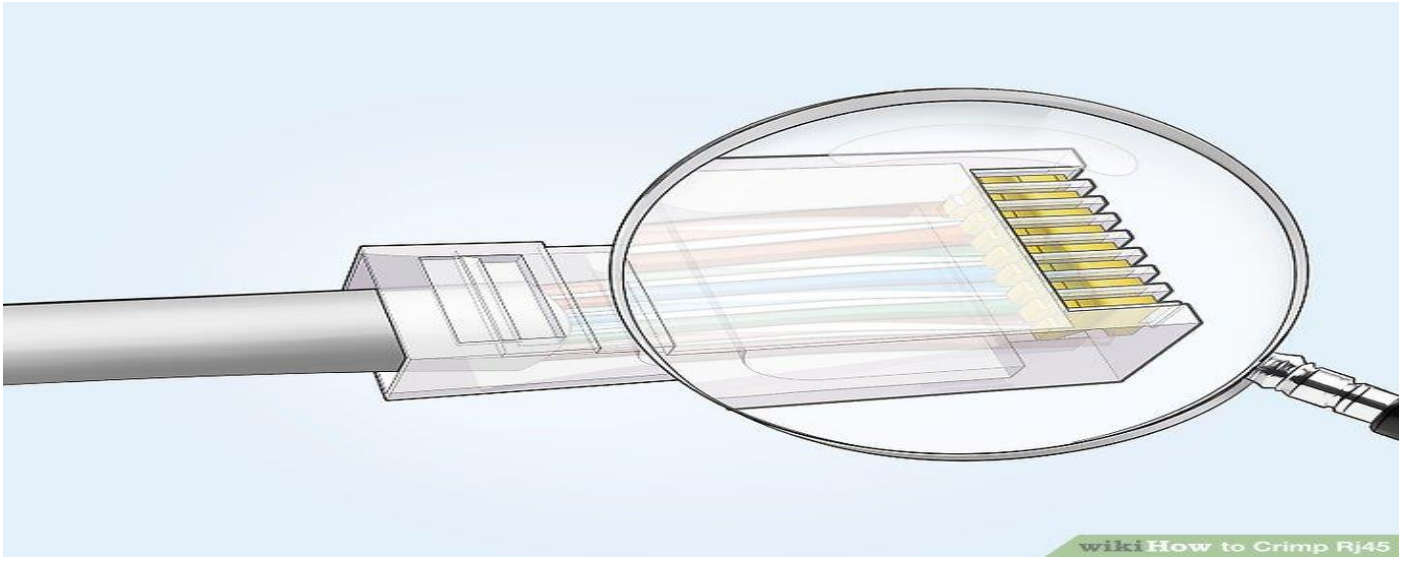
- The sheathing of the cable should fit just inside of the connector so it’s past the base.
- If any of the small wires bend or don’t fit into a groove correctly, take the cable out and straighten the wires with your fingers before trying again.

- The wires must be inserted in the correct order and each wire must fit into a groove before you crimp the connector.



6. Stick the connector into the crimping part of the tool and squeeze twice. Insert the connector in the crimping section of the tool until it can't fit any further. Squeeze the handles to crimp the connector and secure the wires. Release the handles, then squeeze the tool again to make sure all of the pins are pushed down.

- The crimping tool pushes small pins in the grooves down onto the wires to hold and connect them to the RJ-45 connector.

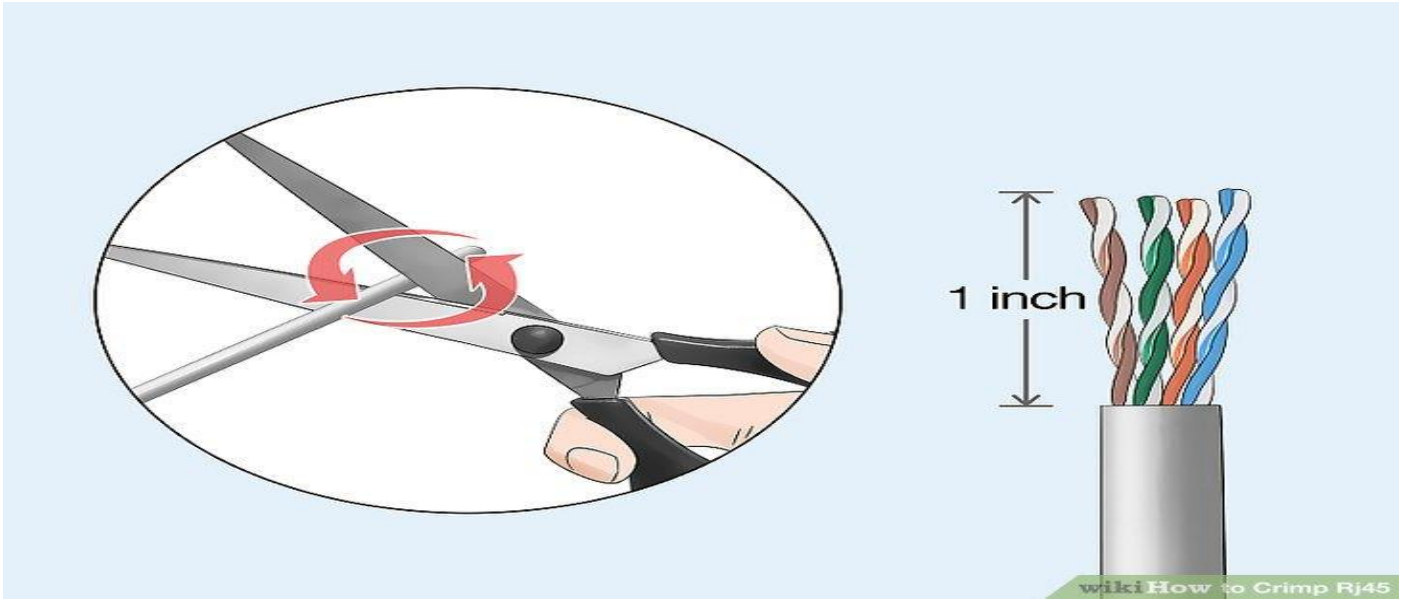


7. Remove the cable from the tool and check that all of the pins are down. Take the connector out of the tool and look at the pins to see that they're all pushed down in an even line. Lightly tug at the connector to make sure it's attached to the cable.

- If any of the pins aren't pushed down, put the wire back into the crimping tool and crimp it again.

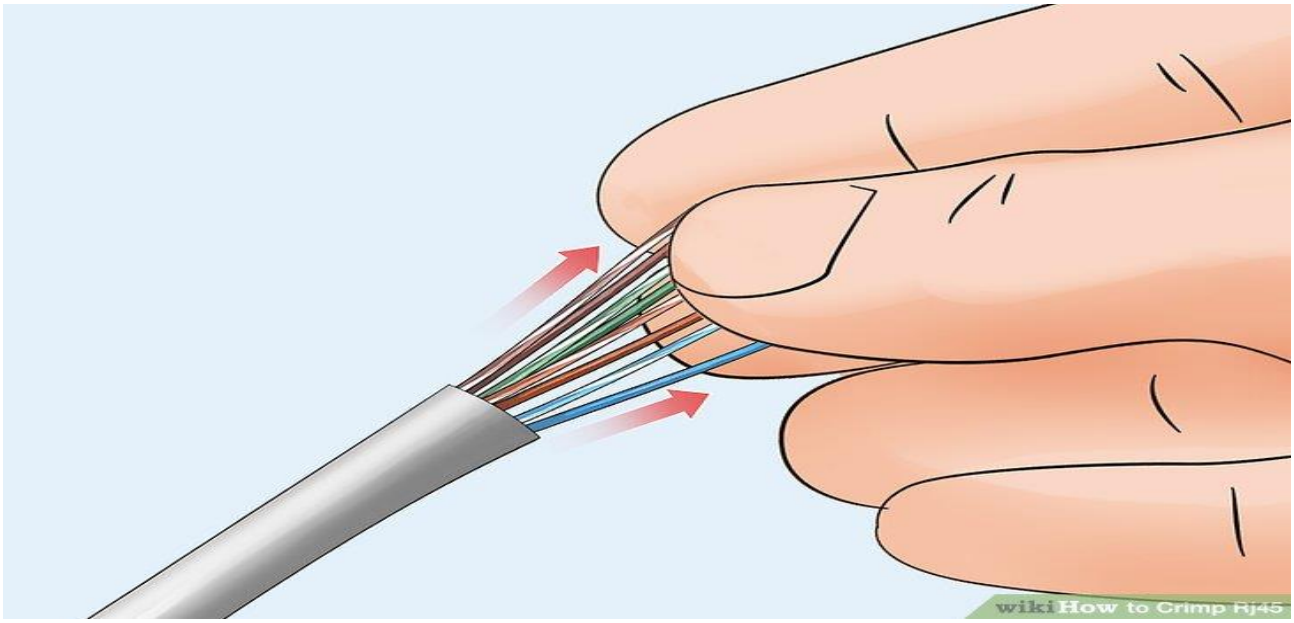
Method2

ATTACHING RJ-45 CONNECTORS WITHOUT A CRIMPING TOOL



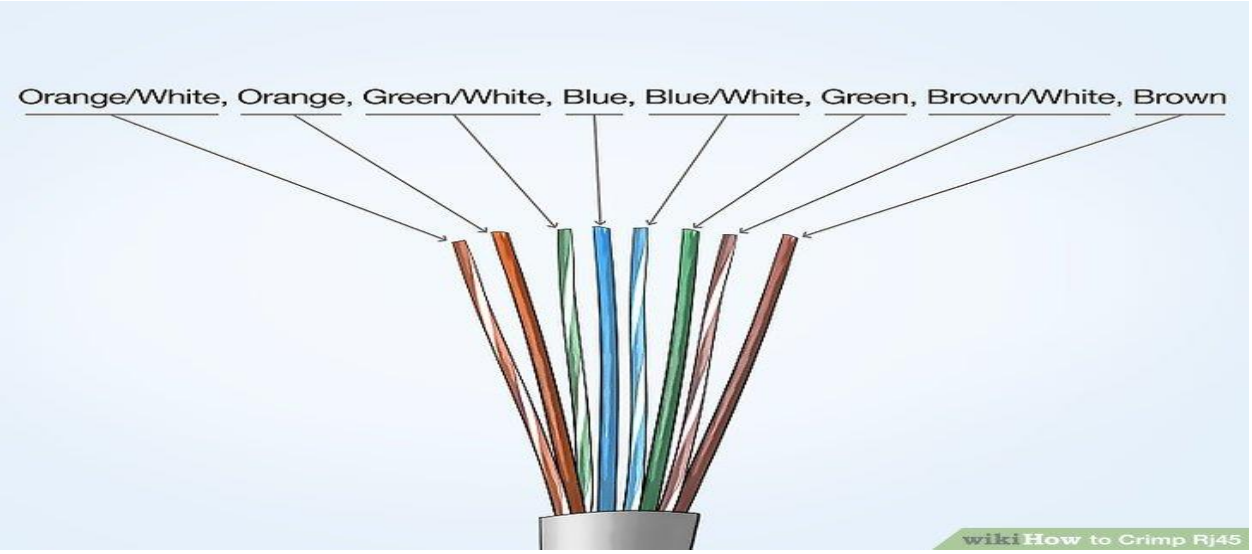
1. Cut into the outer sheath of the cable with a pair of scissors. Take a pair of scissors and gently cut into the plastic sheath about 1 inch (25 mm) from the end of the cable. Make sure you don’t cut into the wires inside. When the scissors penetrate the sheath, rotate the cable and scissors to create a cut around the cable. Then, stick your fingertips under the sheath and pull it off towards the end.
- Don’t cut too deep when you make your initial incision.

Tip: If you don’t have scissors, you can use a utility knife to cut away the outer sheath. But be careful not to cut the wires inside.



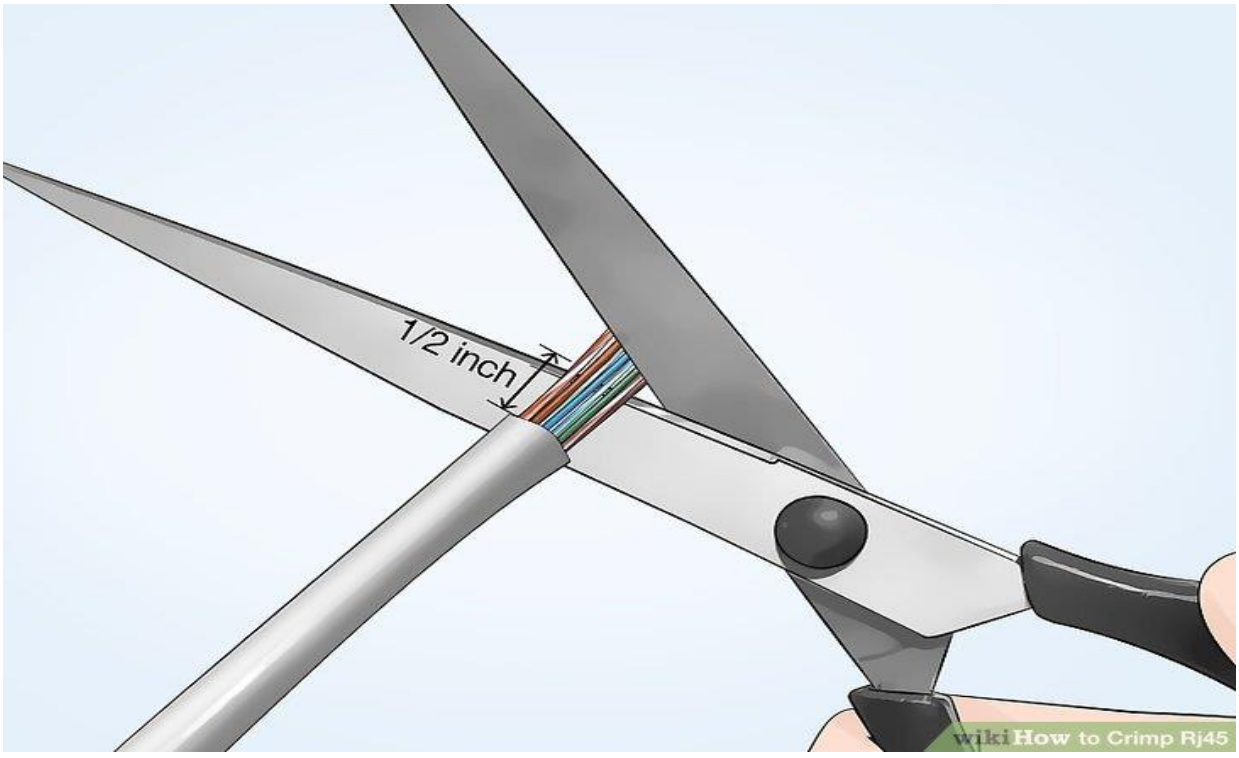
2. Separate and straighten out the small wires in the cable. Use your fingers to untwist and straighten the exposed wires after you remove the sheath. If there is a plastic core

or wire separator, cut it away with your scissors.



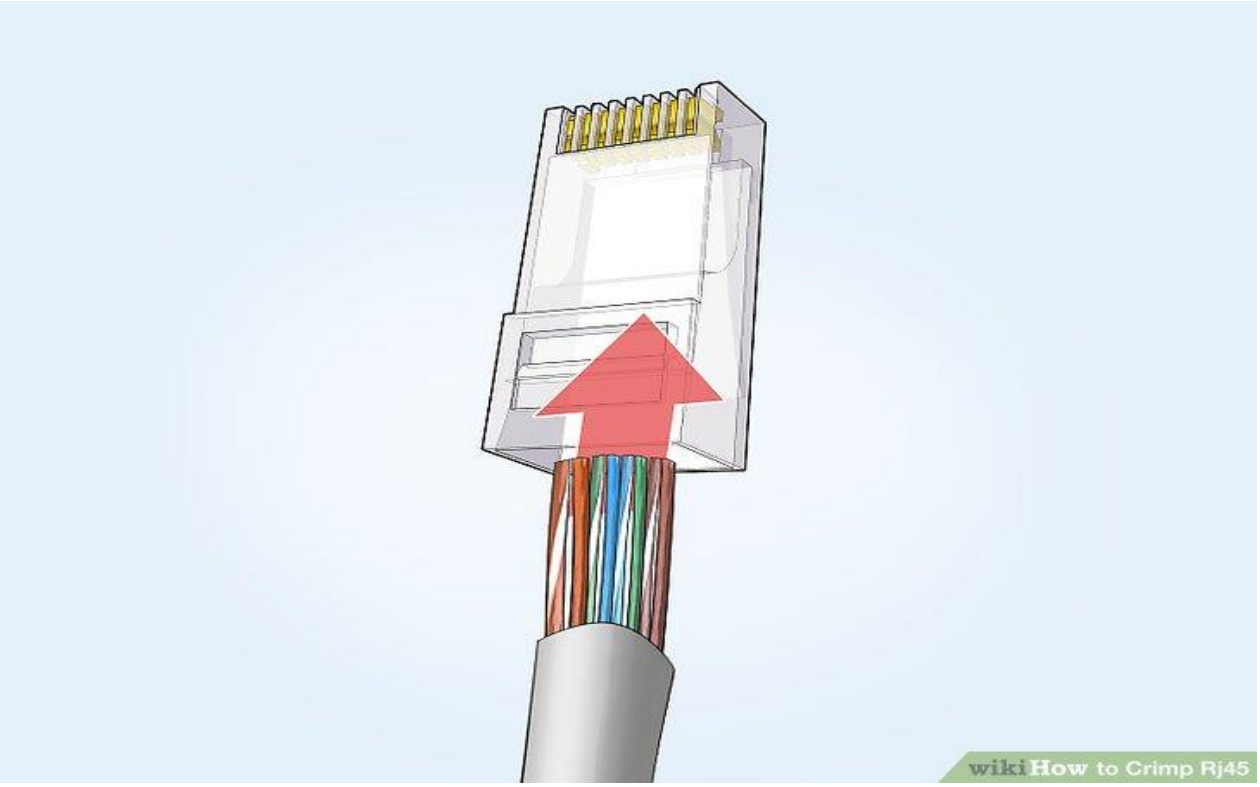
3. Put the wires in the right order. Arrange the wires from left to right so the order is orange/white, orange, green/white, blue, blue/white, green, brown/white, brown. They need to be arranged in a specific order to be properly crimped to the RJ-45 connector.

- Some of the wires have 2 colors on them, like the orange and white wire.

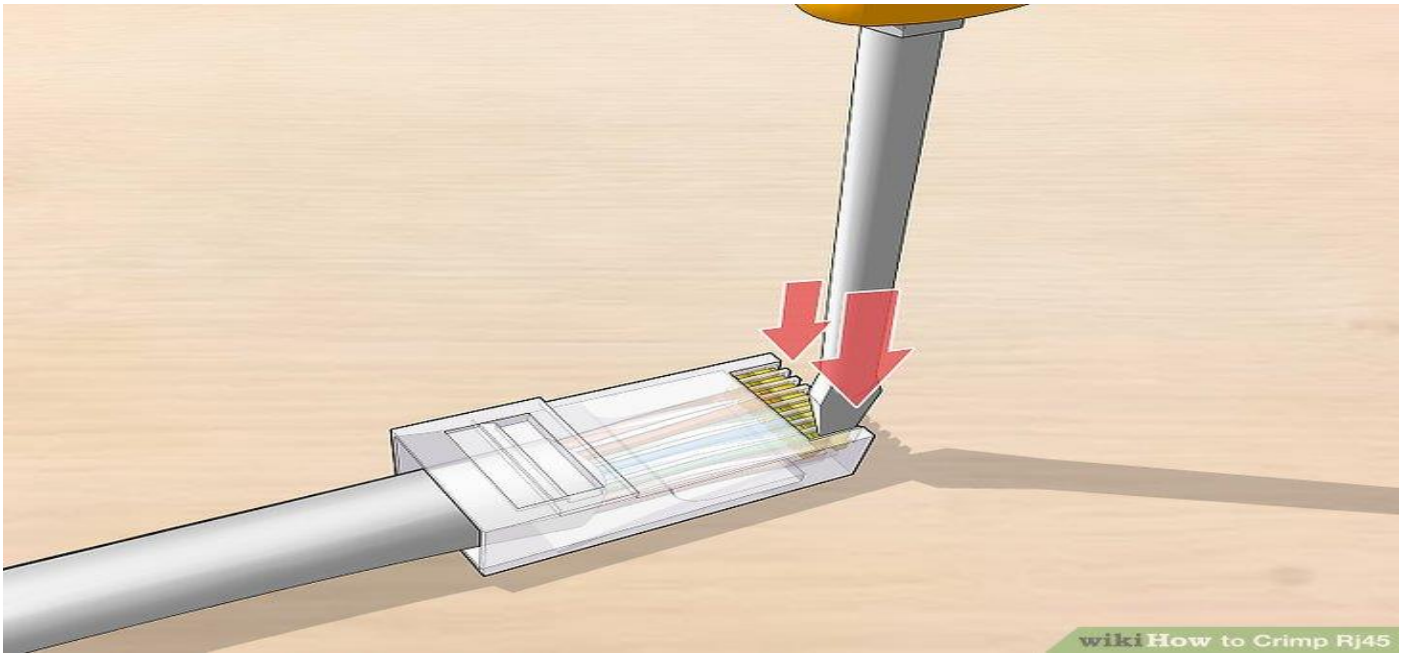


4. Trim the wires ½ inch (13 mm) away from the sheath. Bring the wires together and hold them with your thumb and index finger. Then, use your scissors to cut them. Make sure they're cut evenly.

- The wires need to be even in order to fit into the grooves in the connector.
- If you cut the wires unevenly, move further down and cut them again so their ends are in a straight line.

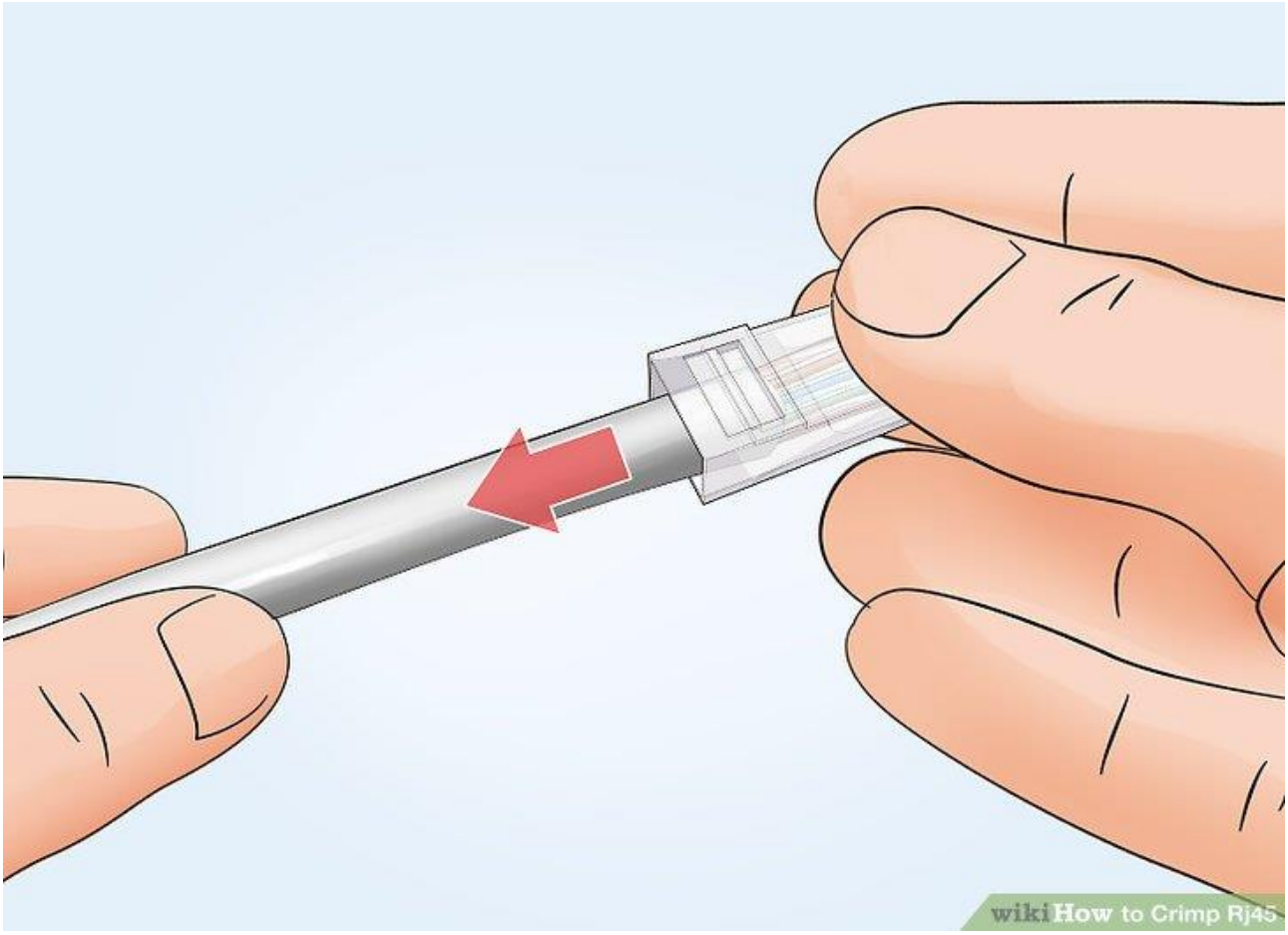


5. Fit the wires into the grooves of the RJ-45 connector. Hold the connector so the metal pins or brackets are facing up and the clip is facing down. Hold the small wires together in the right order and slide them into the connector. They should fit into the grooves of the connector, with the end of the sheath of the cable fitting just past the base of the connector.



6. Press the pins down with a flathead screwdriver. Locate the small metal pins at the ends of the grooves of the connector. Use a thin, flathead screwdriver to push each of the pins down. Push the pins 1 by 1 so they’re pressed all the way into each wire.

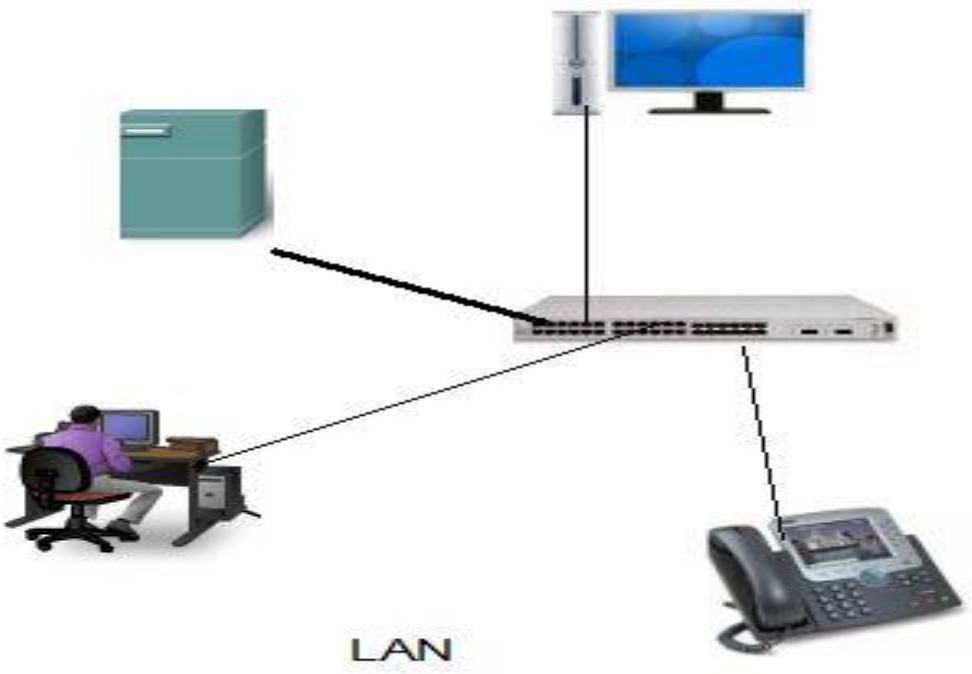
- Be careful not to crack or break the plastic connector.



7. Tug on the end of the connector to make sure it’s secure. Double check that all of the pins are pressed into the wire, and give a light tug on the connector to make sure it won’t slide off. Each of the pins should be inserted at the same level to form an even line.

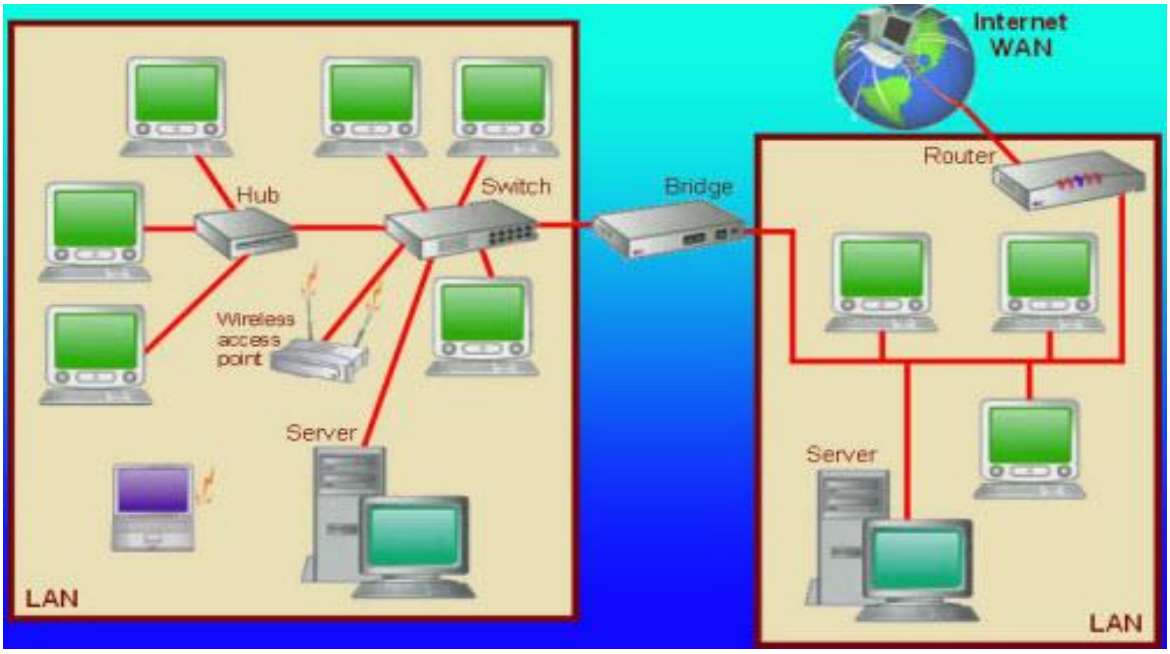
- Lightly shake the cable and listen for any rattling that could indicate that one of the pins isn’t secure.

HOW TO SET-UP A LOCAL AREA NETWORK



Speaking of local area networks, or LANs, they are smaller networks, usually within an office base. LAN is used to connect computing resources, typically inside one building. The computing resources can be computers, printers, servers, IP phones, or routers. Connections between the workstations are physical, with cables, and all the office resources are shared and distributed between the network workstations. The most common type of LAN is that of Ethernet. This is a family of frame-based computer networking technologies for LANs. You must first identify which services you need to provide locally on the LAN. Computers are connected to a switch with Ethernet cables. Each device has a unique IP address.

What You Need While Setting up LAN Network: Cable router, Crossover Ethernet cables, Ethernet cables, Ethernet switch, Network interfaces



INSTRUCTIONS TO SET UP LAN NETWORK

CREATE NETWORK

1. Identify the local services that you want available on the network. Identify network-attached printers, network disk drives, any server that will share printers or disks.

2. Identify how many devices will have to connect to the network. Each device, server or workstation will require a unique address.

3. Run cables to workstations where possible. A wired LAN will always get better performance and be more secure than a wireless LAN. Wherever possible, run a cable to servers, printers, IP phones or work locations. Run a cable to any area where you are likely to work. Use standard Ethernet cables or building wiring as installed according to the TIA-568 standard.

4. Select and purchase a switch or cable router. The simple secure way to connect to the Internet is to use a cable router. Many makes and models are available. If the model you choose does not have enough ports to connect all of your computers, then you will need to purchase a switch as well.

5. Configure the WAN port of the cable router. Configuration details will vary from vendor to vendor. Key information you will need to configure the WAN port will be supplied by your internet service provider.

6. Configure the LAN ports of your cable router. Most cable routers will act as a Dynamic Host Configuration Server, or DHCP server. This means that the router will give addresses to workstations automatically. Be certain that the address pool has enough addresses for all of the workstations. Make certain that there are enough addresses outside of the range for any hosts that need static addresses. For example, a network address with a mask of 255.255.255.0 has a total of 254 hosts. If the dynamic pool has 200 addresses available, that means the remaining 54 addresses are available to give printers or servers static addresses.

7. Connect the wires for the network. Workstations and servers can be connected with standard Ethernet cables. Connect the switch to the cable router LAN ports by using the up-link or straight port on the switch. If the switch does not have an up-link port, connect any standard port of the switch to a LAN port on the cable router with an Ethernet crossover cable. Ethernet crossover cables can be purchased at any electronics store.

8. Test the services and Internet connectivity. Test each of the workstations to ensure they can connect to the Internet and test any local servers and printers. Print test pages on the shared printers. Tests read and write permissions on shared file servers by copying files to the servers and copying files from the server to a workstation.

TIPS & WARNINGS

- Purchase a cable router with wireless capabilities to give you more flexibility.
- Make sure cable lengths do not exceed 100 meters, or about 300 feet.
- Do not run cables in air ducts unless they are fire rated. Check local building codes.

Tips: The differences between LAN and WAN are stated in tabular form below:-

	LOCAL AREA NETWORKS (LANS)	**WIDE AREA NETWORKS (WANS)**
MOST COMMONLY:	Ethernet, Token Ring, FDDI	Leased lines, serial links, ISDN, X.25
ADVANTAGE:	Speed	Distance
COST CENTER:	dense installation (about one interface per room)	length of long-haul lines (about one interface per 100 miles)
CURRENT SPEED:	10-100 Mbps (mostly 10 Mbps)	0.01 to 45 Mbps (mostly clustered around 1 Mbps)
COMMON USES:	File sharing	Email and file transfer (including Web)
COMMON PROBLEMS:	Cable disruption by users	Cable disruption by backhoes
CONCEPTUALLY:	A bunch of lines hooking users together	A bunch of lines hooking cities together

PRACTICAL ILLUSTRATIONS AND DIAGRAMS ON HOW TO CREATE LOCAL AREA NETWORK (LAN)

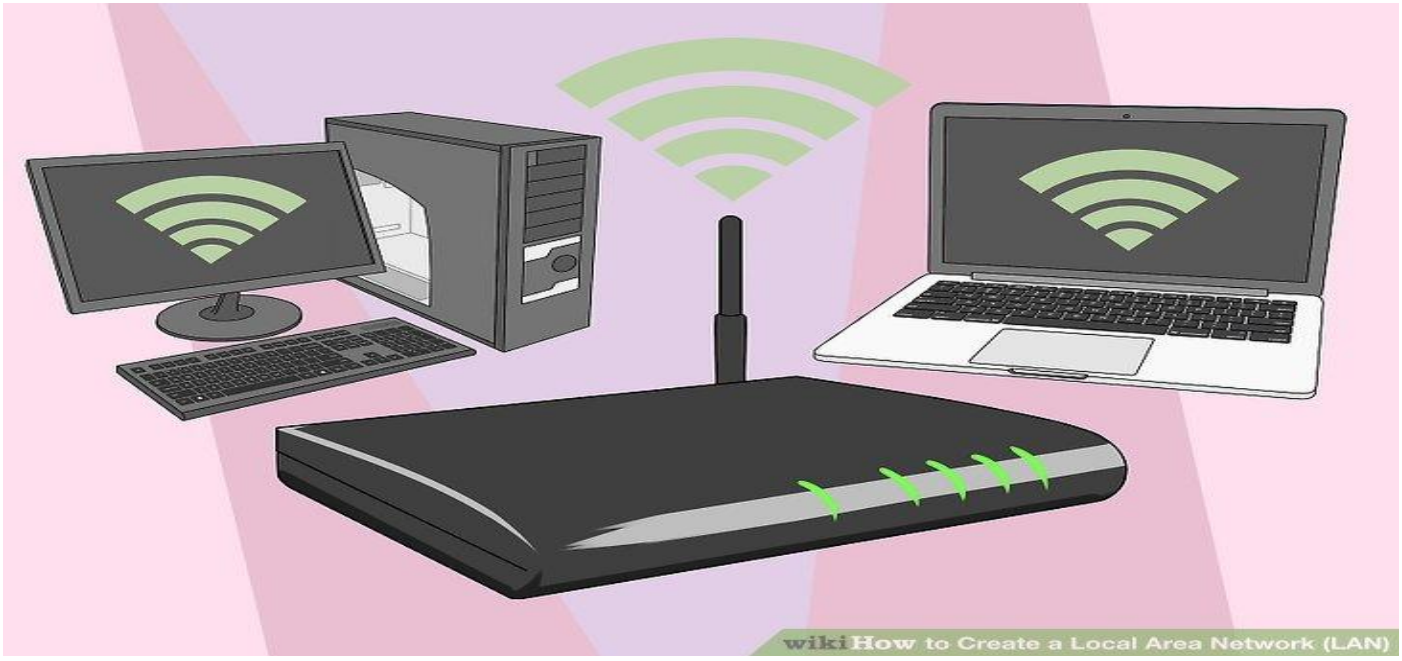
Part1

DETERMINING YOUR NETWORK NEEDS

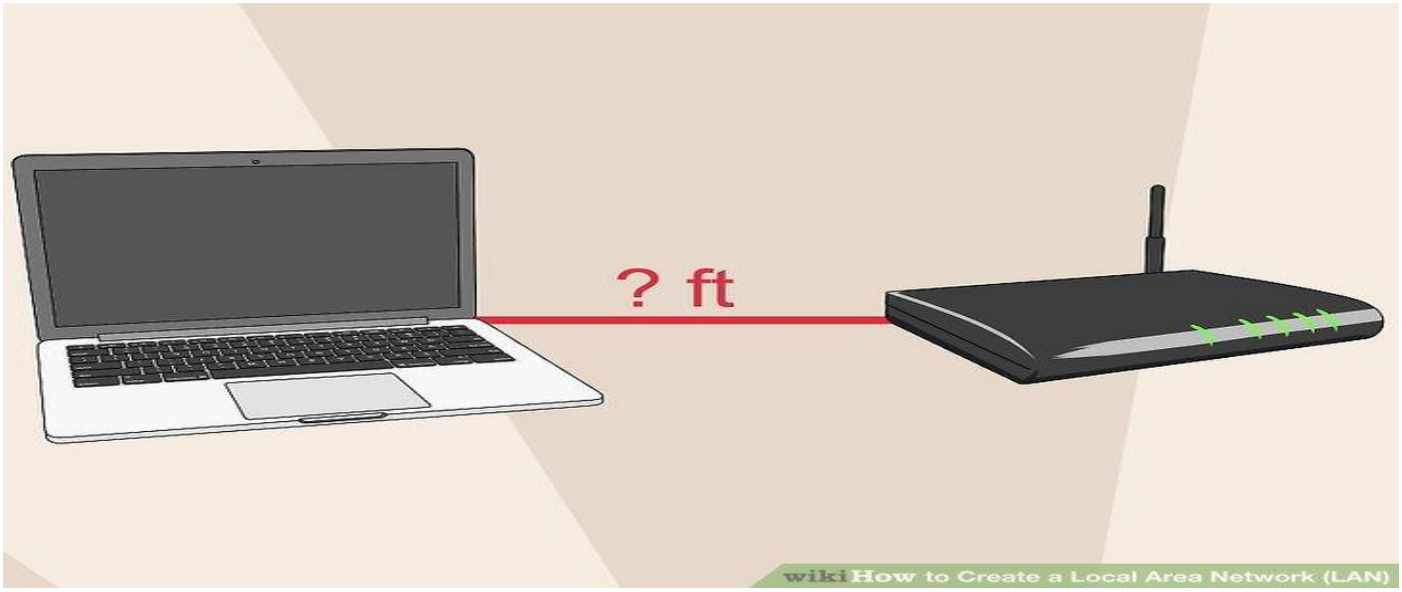
1. Count the number of computers you need to hardwire. When setting up a LAN, you'll need to know how many computers will be connecting to the network via Ethernet. This will determine the number of ports you'll need.
   If you have four or less computers that you need to hardwire, you'll just need a router.
   If you have more than four, you'll likely need to get a switch to extend the number of ports available on your router.

2. Decide if you want to create a wireless network. If you want to allow devices to connect wirelessly, you'll need a router that can broadcast a wireless network. Most routers you'll find at the store or online have wireless capabilities.

- Network switches do not allow wireless devices to connect, and can only be used for hardwired LANs or to extend the number of ports available to the router.



3. Determine if you want all network devices to have internet access. If you want all of the connected devices to have access to the internet, you'll need a router to handle the connections. If you don't need the devices to have a network connection, you can just use a network switch.

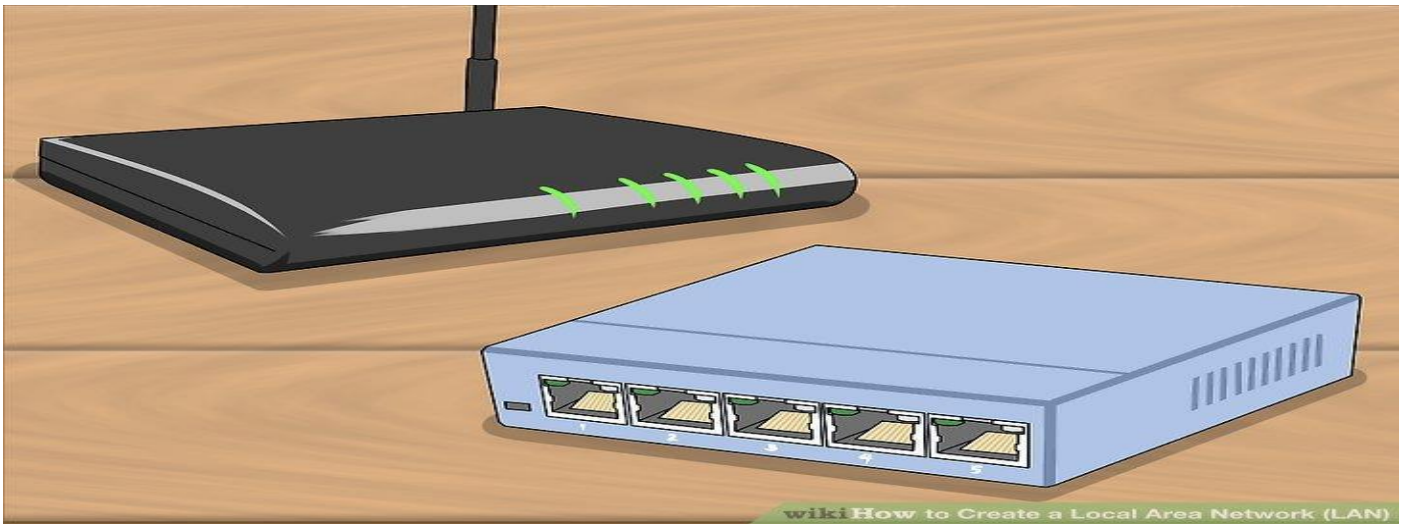


4. Measure the distances for all hardwired devices. This isn't much of an issue in most homes, but network cables cannot run longer than 100m (328 ft). If you have to run cable farther than this, you'll need switches in between.

5. Consider your future needs. If you're filling all of the ports on your hardware, consider future-proofing to allow for more devices in the future.

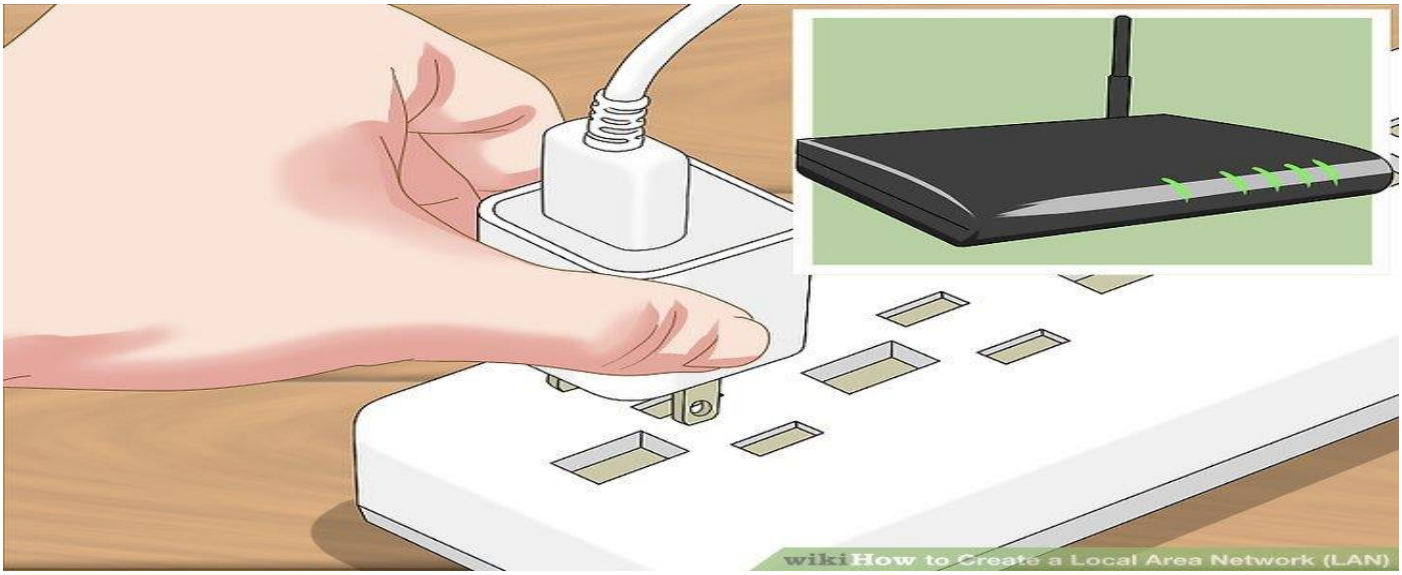
Part2

SETTING UP A BASIC LAN

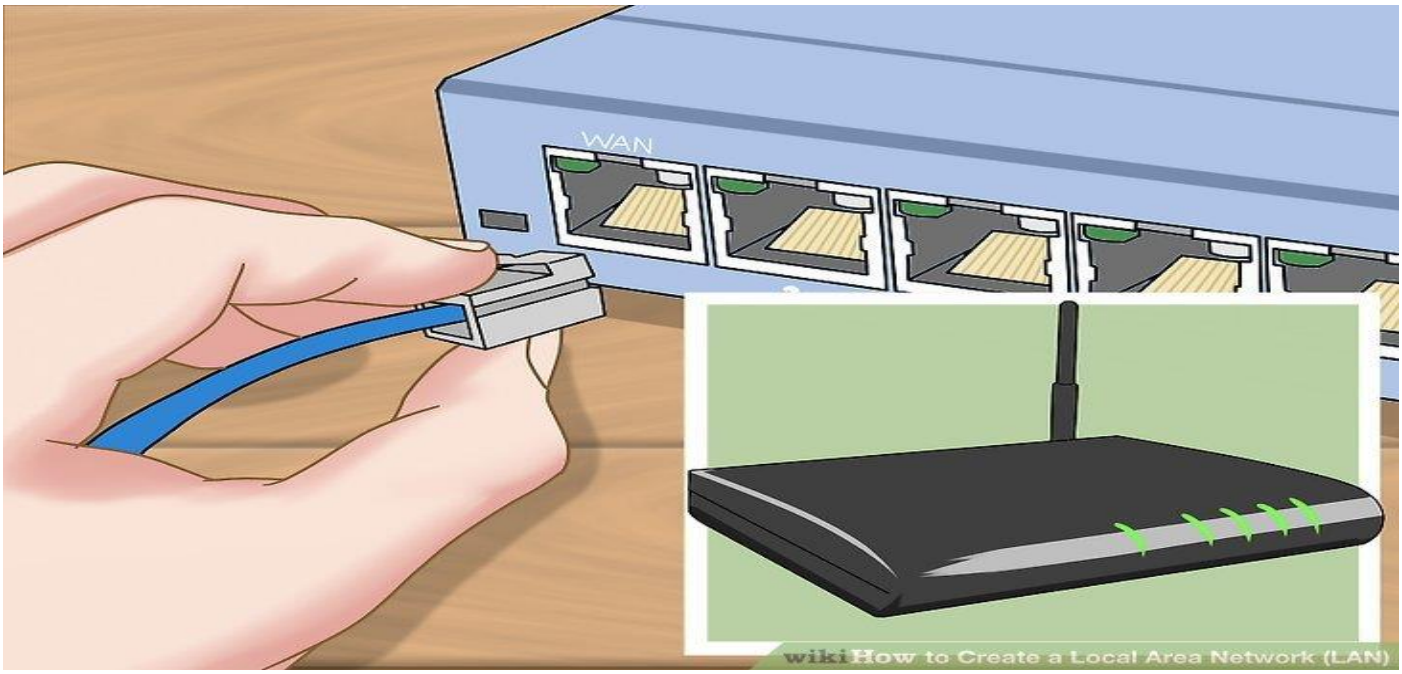


1. Gather your network hardware. To create a LAN, you'll need a router or switch, which will act as the hub of your network. These devices route information to the correct computers.

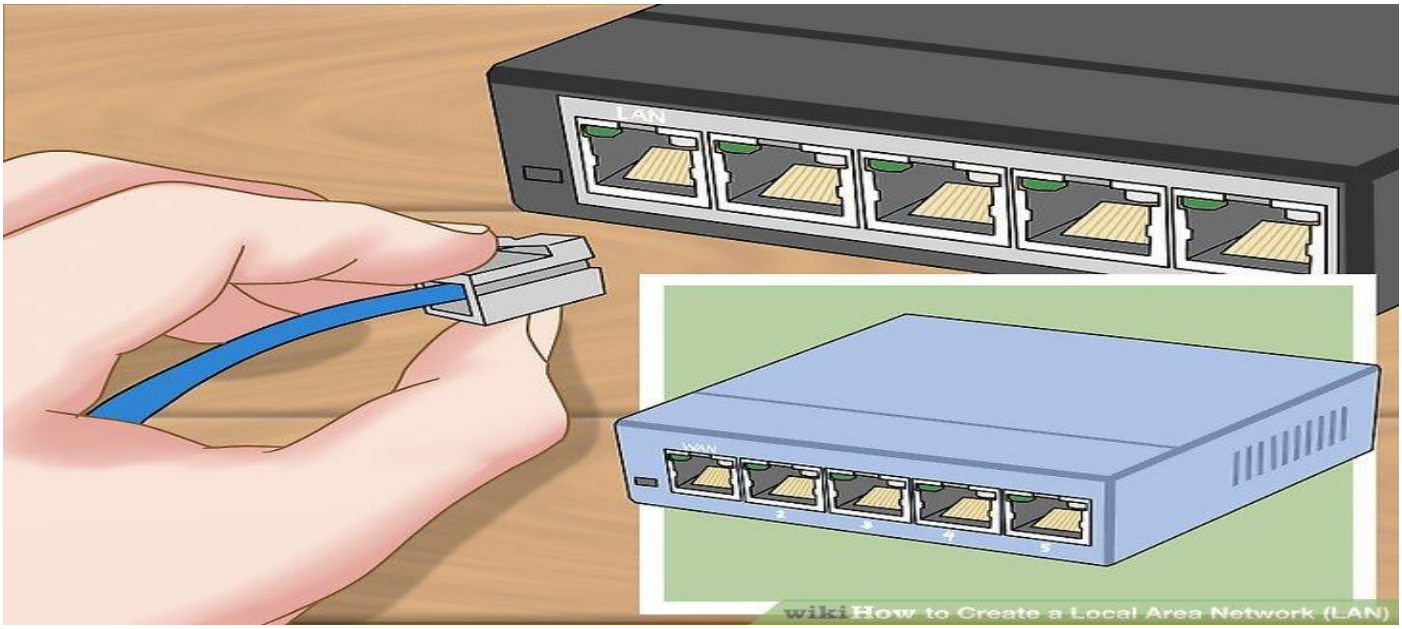
- A router will automatically handle assigning IP addresses to each device on the network, and is necessary if you intend to share your internet connection with all the connected devices. It is highly recommended that you build your network with a router, even if you're not sharing an internet connection.
- A network switch is like a simpler version of a router. It will allow connected devices to talk to each other, but will not automatically assign IP addresses and will not share an internet connection. Switches are best used to expand the number of LAN ports available on the network, as they can be connected to the router.



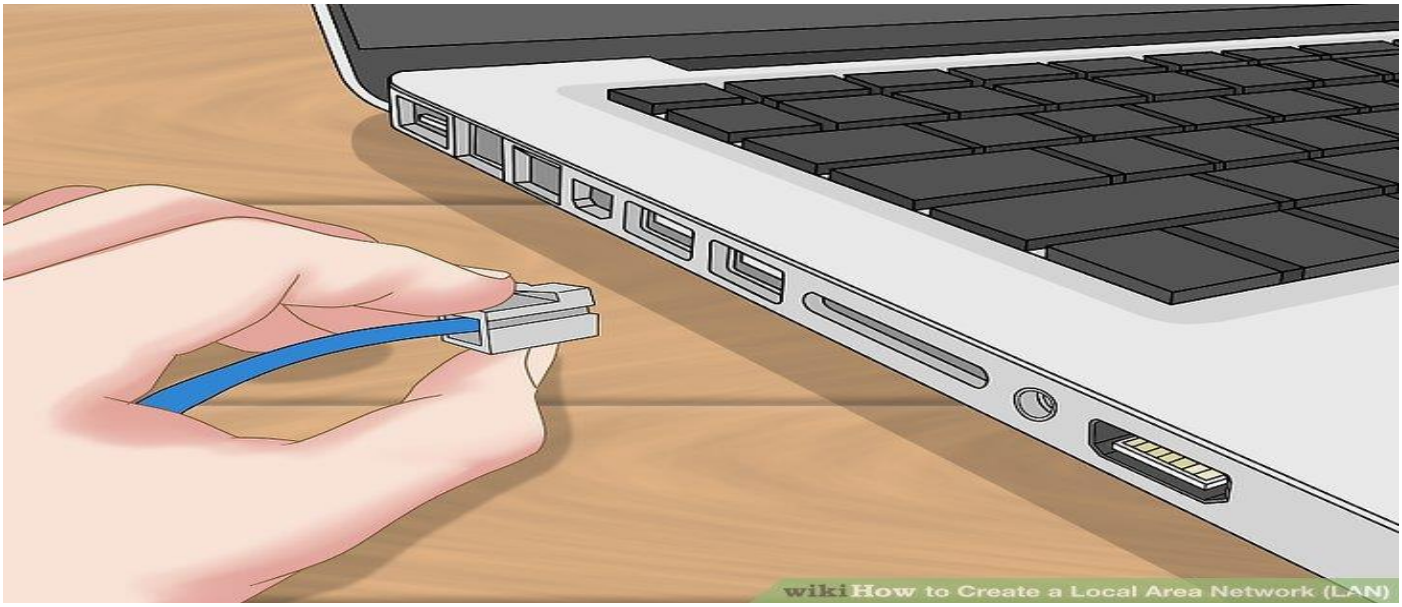
2. Set up your router. You don't need to do much to set up a router for a basic LAN. Just plug it into a power source, preferably close to your modem if you plan on sharing the internet connection through it.



3. Connect your modem to your router (if necessary). If you're sharing the internet connection from your modem, connect the modem to the WAN/INTERNET port on the router. This is usually a different color from the other ports.

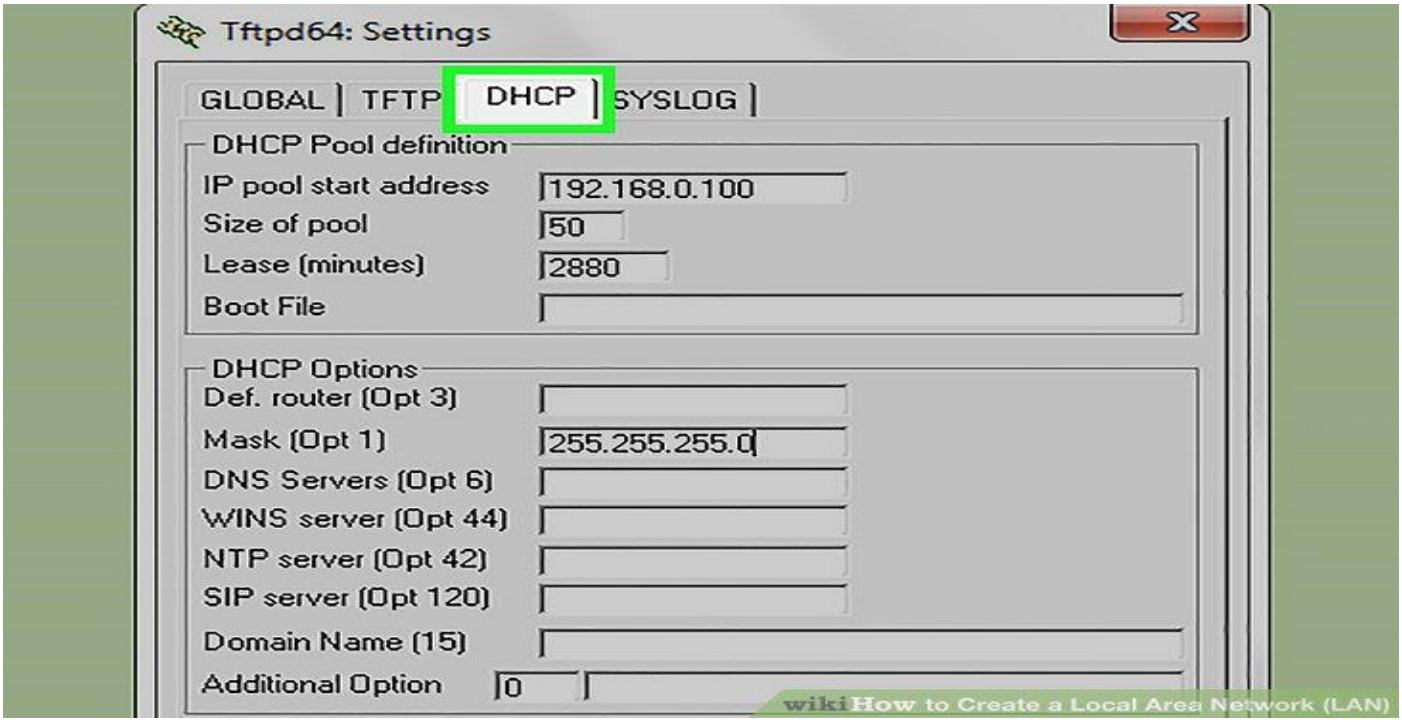


4. Connect your switch to your router (if necessary). If you're using a switch to expand the number of ports available on the router, plug an Ethernet cable into any LAN port on the router and any LAN port on the switch. This will expand the network to the rest of the LAN ports on the switch.



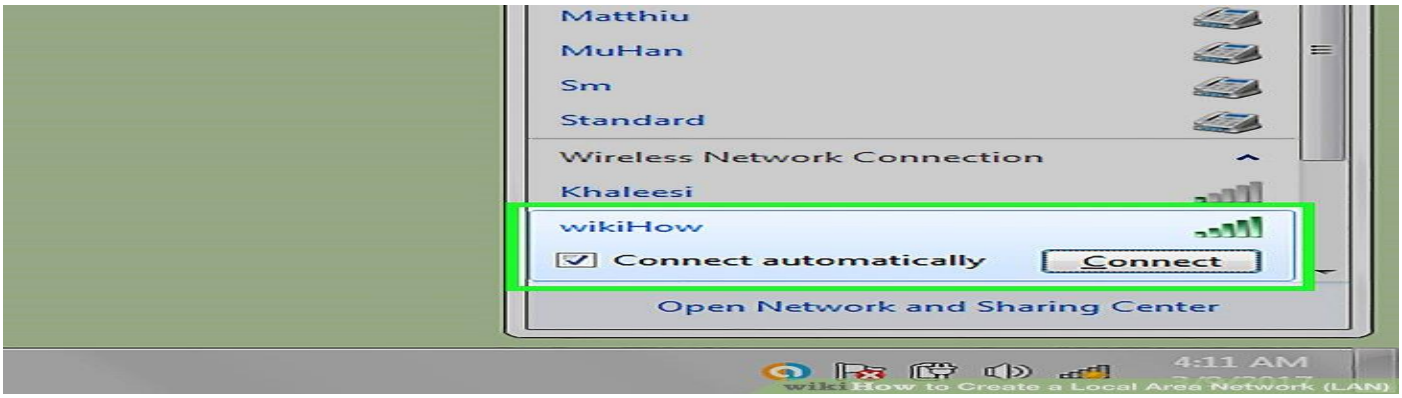
e5. Connect your computers to open LAN ports. Use Ethernet cables to connect each computer to an open LAN port on your router or switch. It doesn't matter what order the ports are connected in.

•Ethernet cables cannot reliably transfer data at lengths larger than 100m (328 ft).

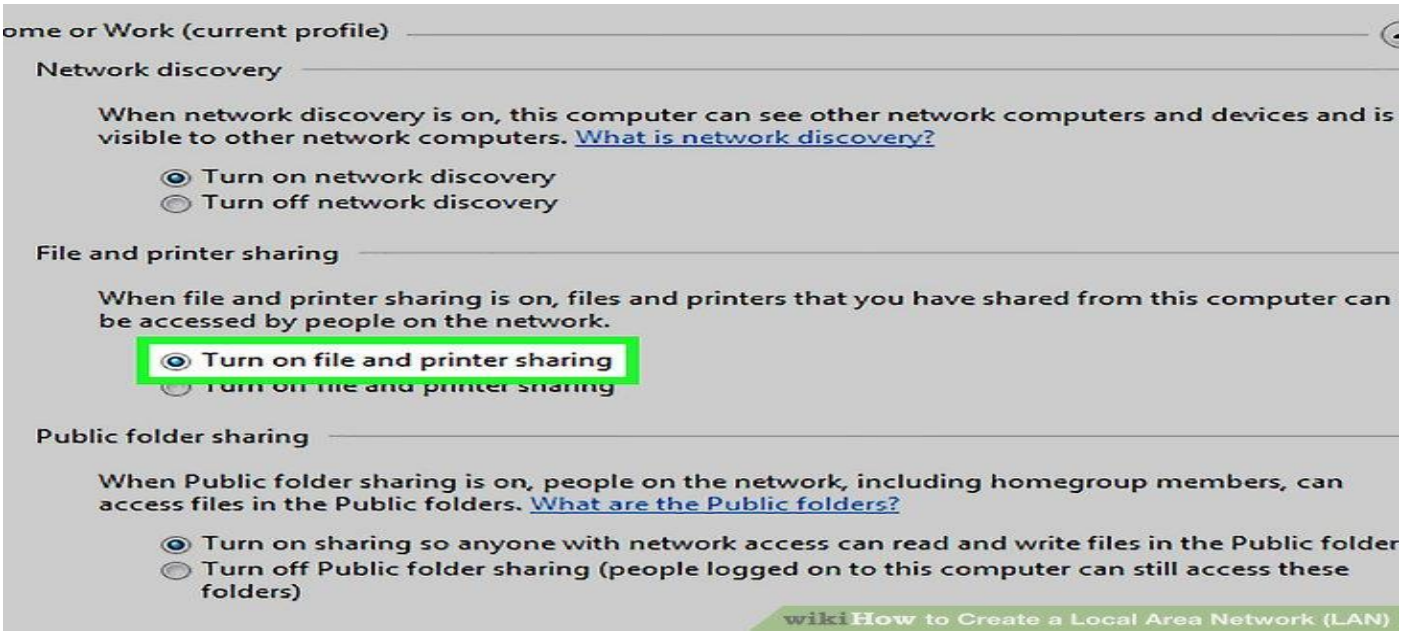


6. Setup one PC as a DHCP server if you're just using a switch. If you're only using a switch as your network hub, setting up one computer as a DHCP (Dynamic Host Configuration Protocol) server will allow all of the connected computers to easily obtain IP addresses.

- You can quickly create a DHCP server on one of your computers by installing a third-party utility.
- The rest of the computers on the network will obtain IP addresses automatically once the server is running, as long as they are set to do so.



7. Verify the network connection on each computer. After each computer obtains an IP address, they'll be able to talk to each other on the network. If you're using a router to share your internet connection, each computer will be able to access the internet.

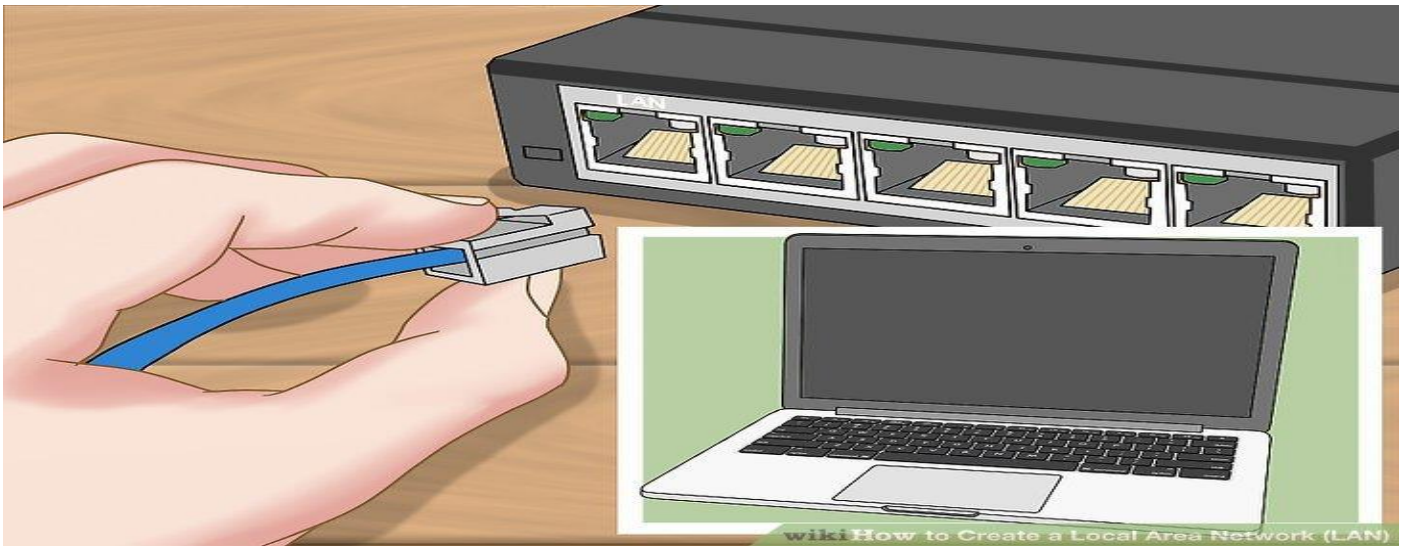


8. Set up file and printer sharing. Once your network is up, you won't see anything on other computers unless that computer has shared files. You can designate files, folders, drives, printers, and other devices as shared so that anyone on the network, or just specific users, can access them.

Part 3

CREATING A WIRELESS NETWORK

1. **SET UP YOUR ROUTER.** When you're setting up a wireless router, you'll need to keep a few things in mind:
   - For easy troubleshooting, the router should usually be placed close to your modem.
   - It should be located centrally to allow for maximum wireless coverage.
   - You'll need to connect a computer to the router via Ethernet during the setup process.



2. **PLUG A COMPUTER INTO ONE OF THE ROUTER'S LAN PORTS.** You'll be using your computer's web browser to configure the router's wireless network.

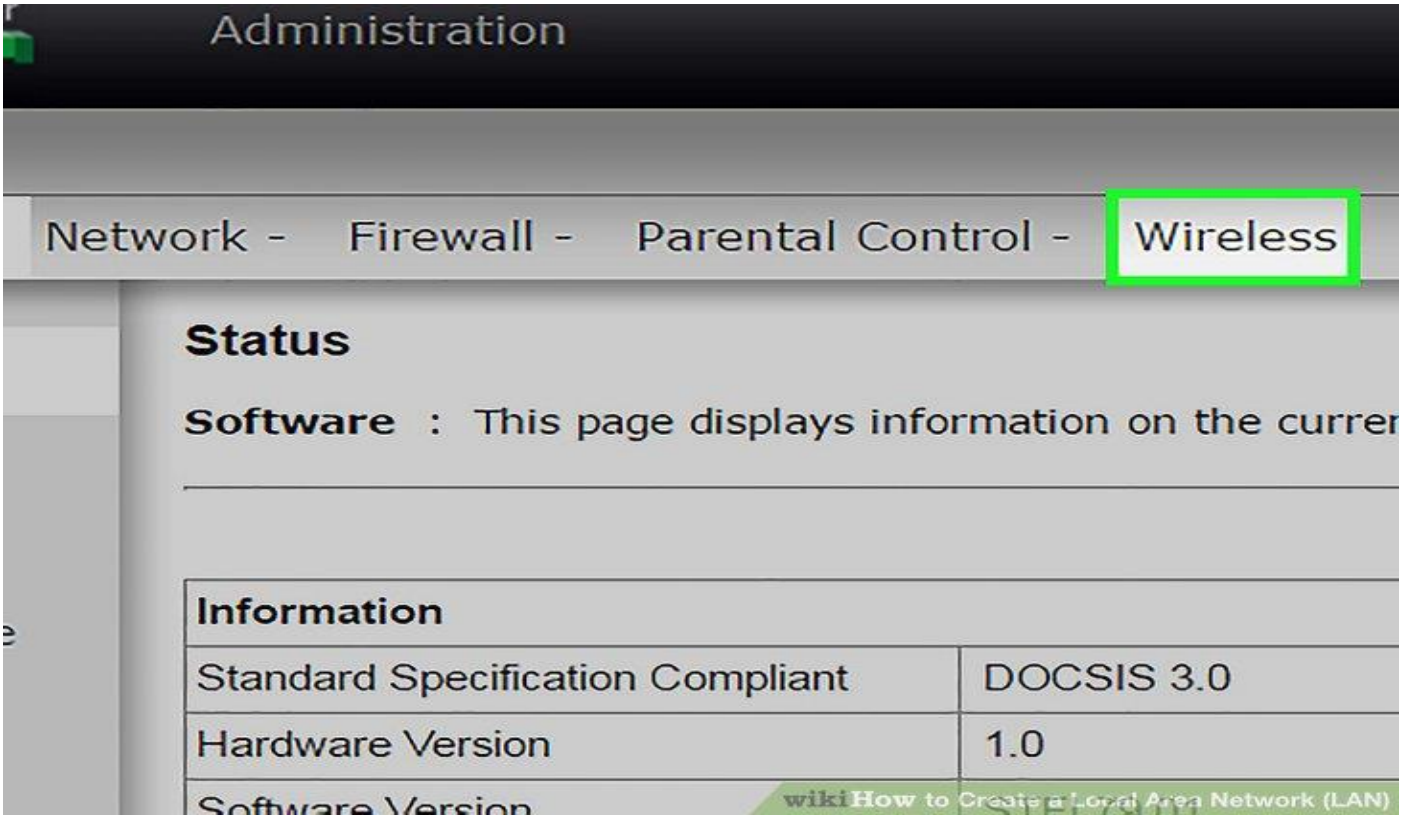
3. OPEN A WEB BROWSER ON YOUR COMPUTER. You can use any web browser.

4. Type in the router's IP address. You can typically find this printed on the bottom of the router, or in your router's documentation. If you can't find it, there are a couple things you can try:

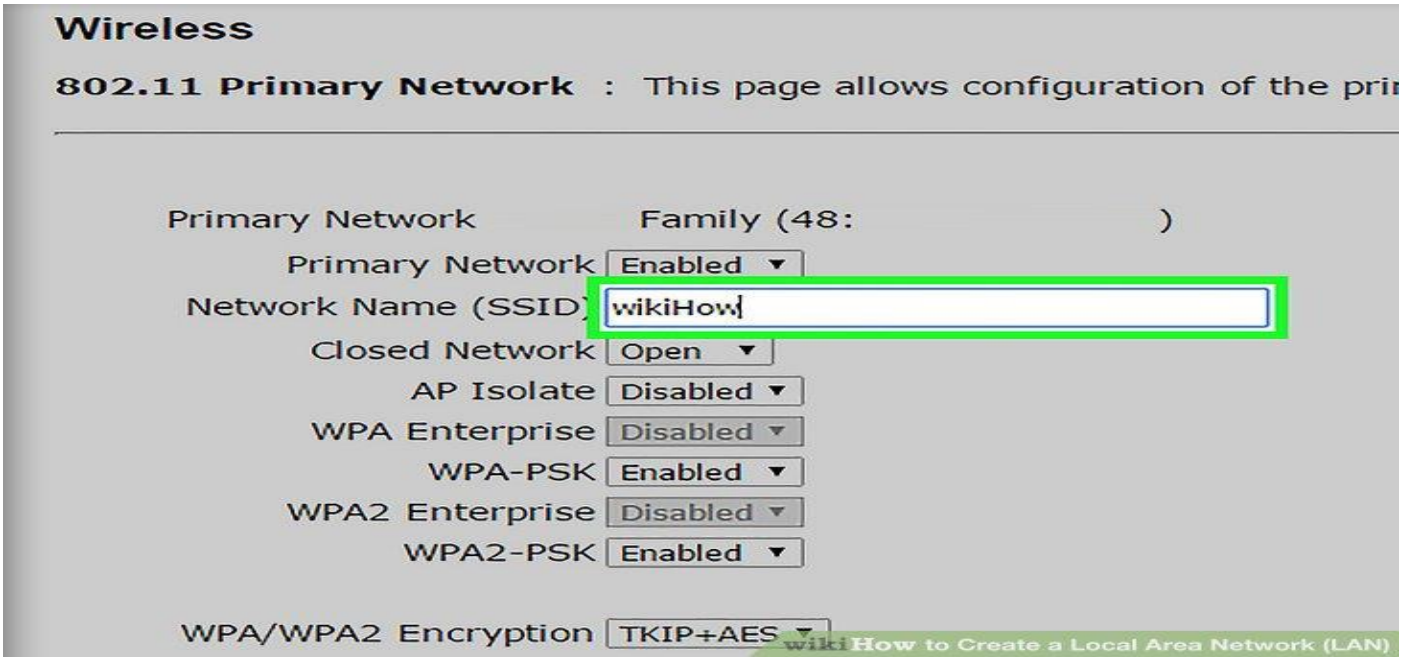
- Windows - Right-click the Network button in the System Tray → click Open Network and Sharing Center → click the Ethernet link → click Details → find the Default Gateway entry for your router's IP address.
- Mac - Click the Apple menu and select System Preferences → click Network → click your Ethernet connection → find the Router entry for your router's IP address.

5. **Log in with the administrator account.** You'll be prompted for the login information for your router. The default login information varies depending on your router model, but the username is often "admin" and the password is often "admin," "password," or blank.

- You can look up your router model at https://portforward.com/router-password/ to find the default login information.

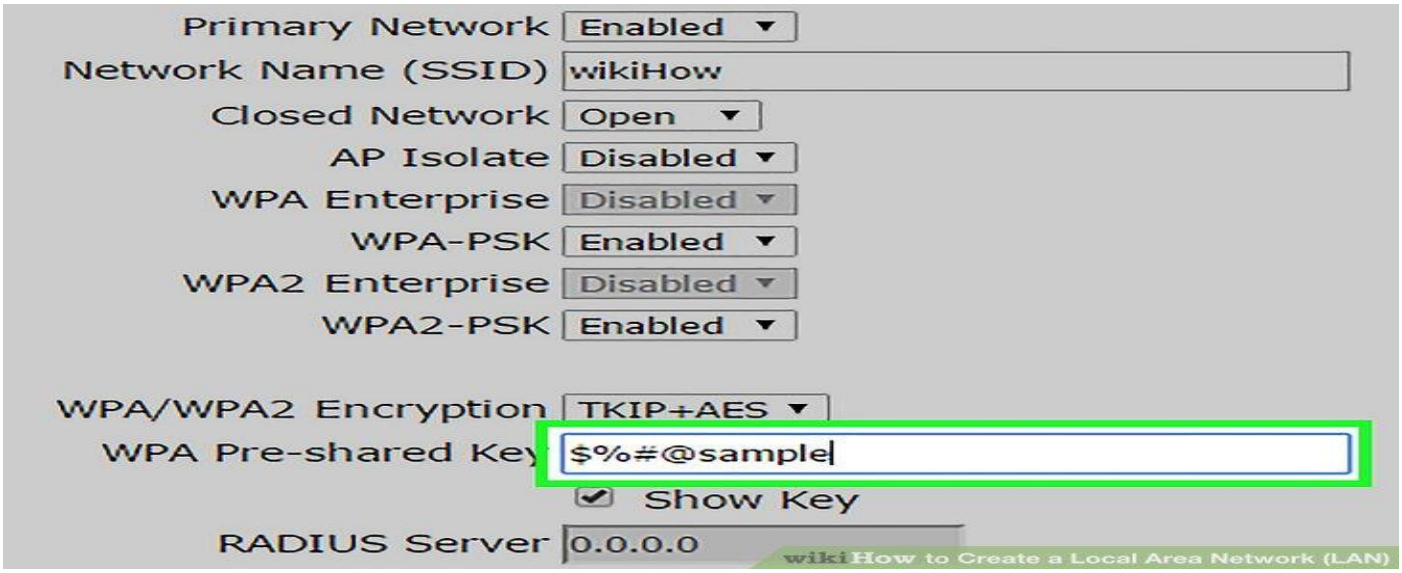


6. OPEN THE WIRELESS SECTION OF THE ROUTER SETTINGS. The exact location and wording of this section varies from router to router.

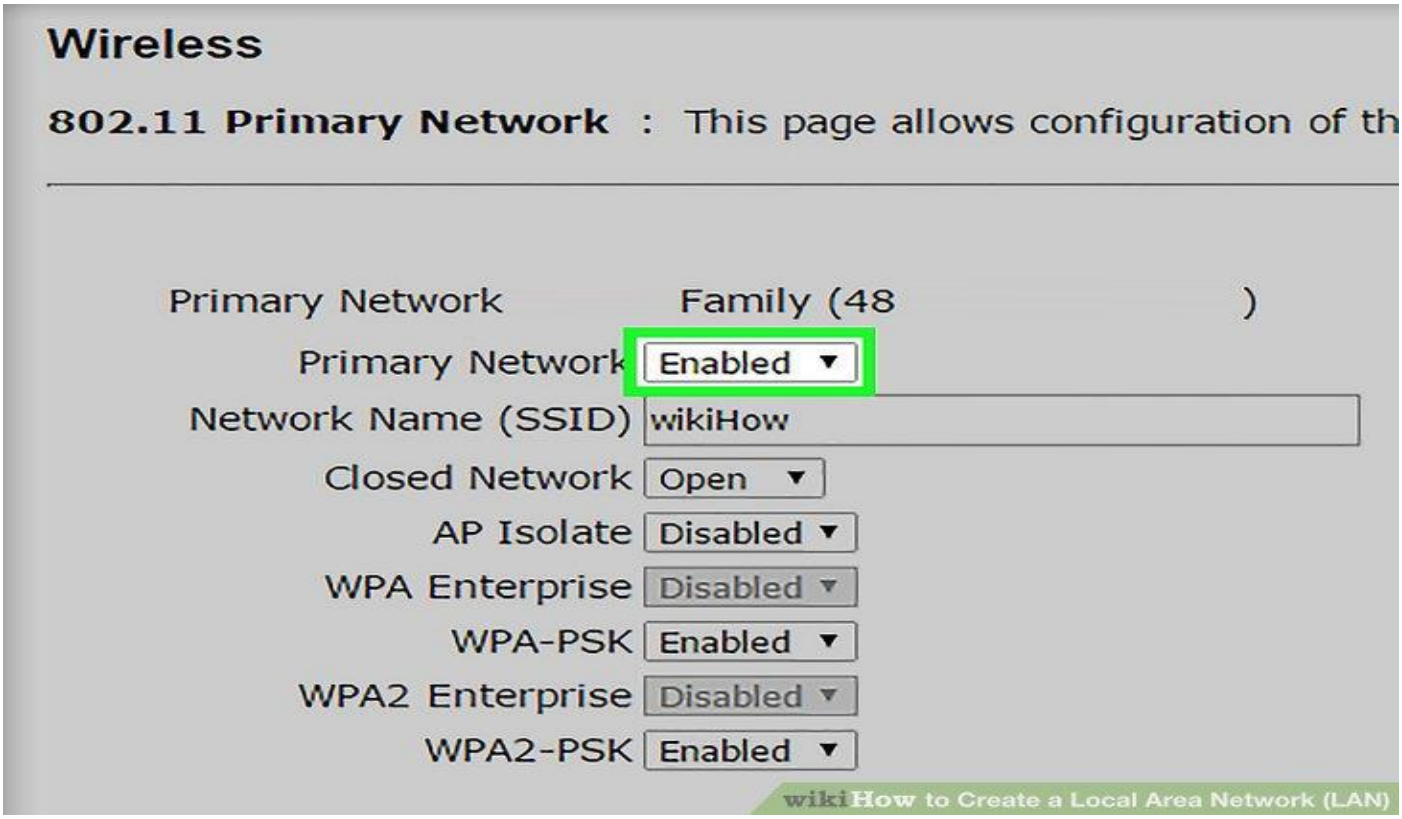


7. CHANGE THE NAME OF YOUR NETWORK IN THE SSID FIELD. This may also be called "Network name." This is the name that appears in the list of available wireless networks.

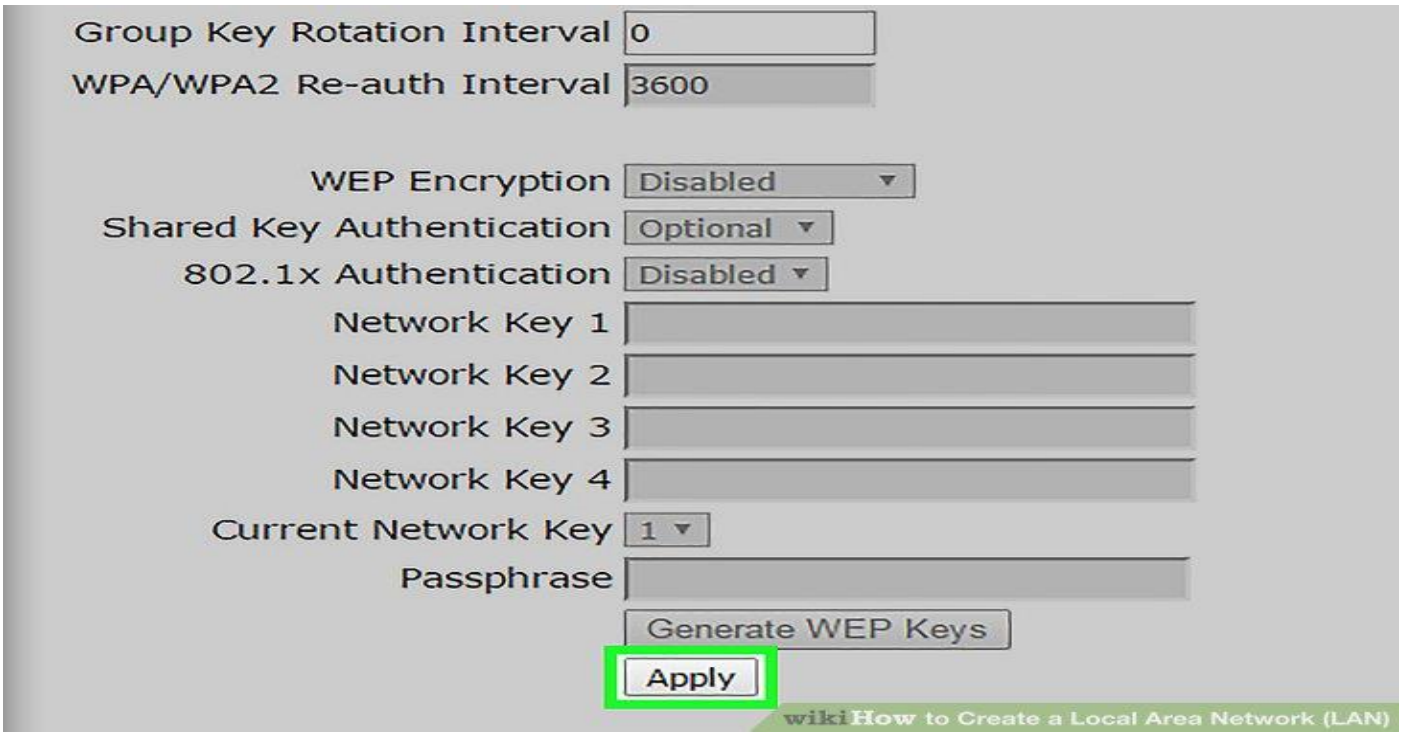
8. SELECT WPA2-PERSONAL AS THE AUTHENTICATION OR SECURITY OPTION. This is the most secure option currently available on most routers. Avoid WPA and WEP except when explicitly required by older, incompatible devices.



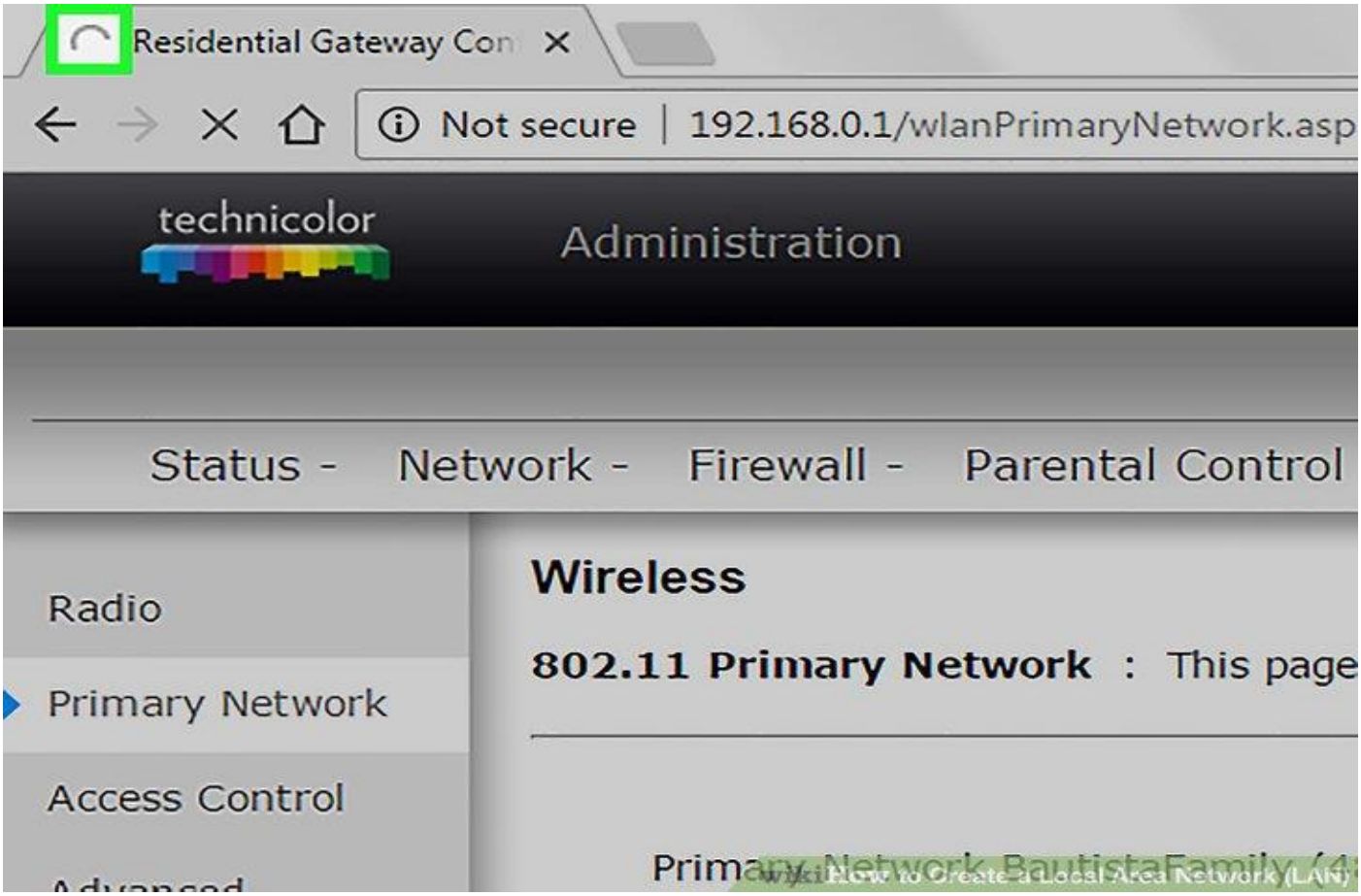
9.CREATE A STRONG PASSWORD. This password will be required in order to connect to the network. The field may be labeled "pre-shared key."



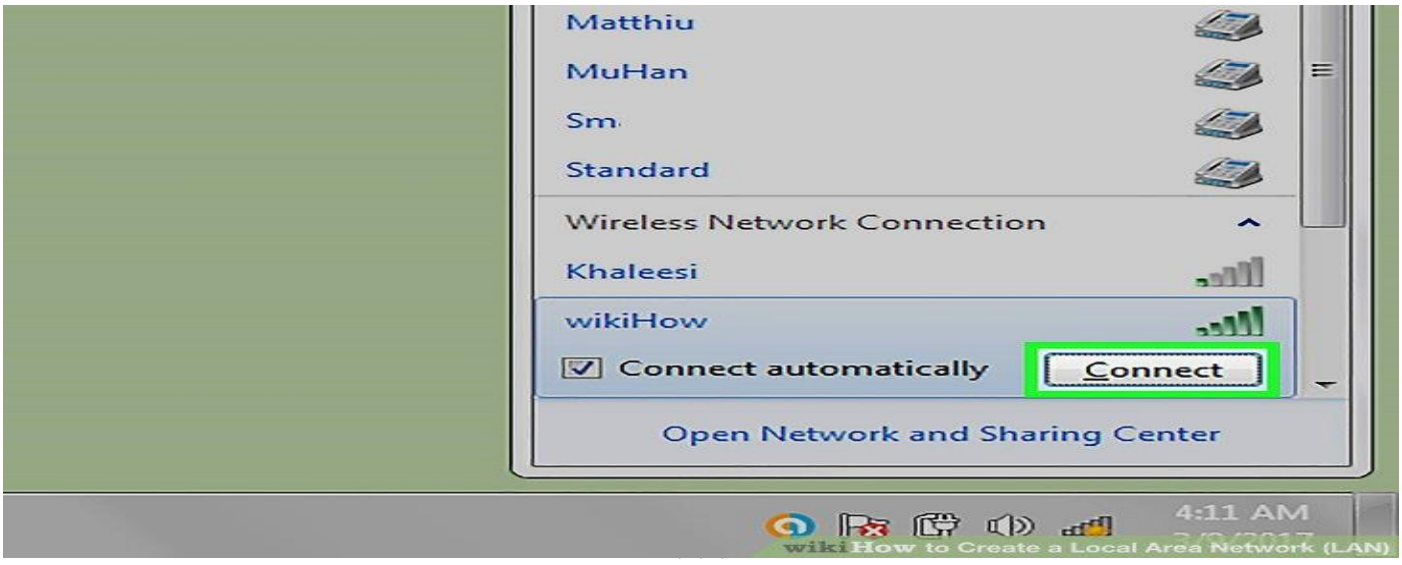
10.ENSURE THE WIRELESS NETWORK IS ENABLED. Depending on the router, you may have to check a box or click a button at the top of the Wireless menu to enable the wireless network.



11.CLICK THE SAVE OR APPLY BUTTON. This will save the changes to your router.



12.WAIT WHILE YOUR ROUTER RESTARTS. It may take a minute for the router and network to come back online.



13. CONNECT TO THE WIRELESS NETWORK ON YOUR WIRELESS DEVICES. Once the network is back up, it will appear on the available network list on any wireless devices in range. When connecting to the network, users will be prompted to enter the password you created.

- Computers connected to the router via Ethernet will not require a password.